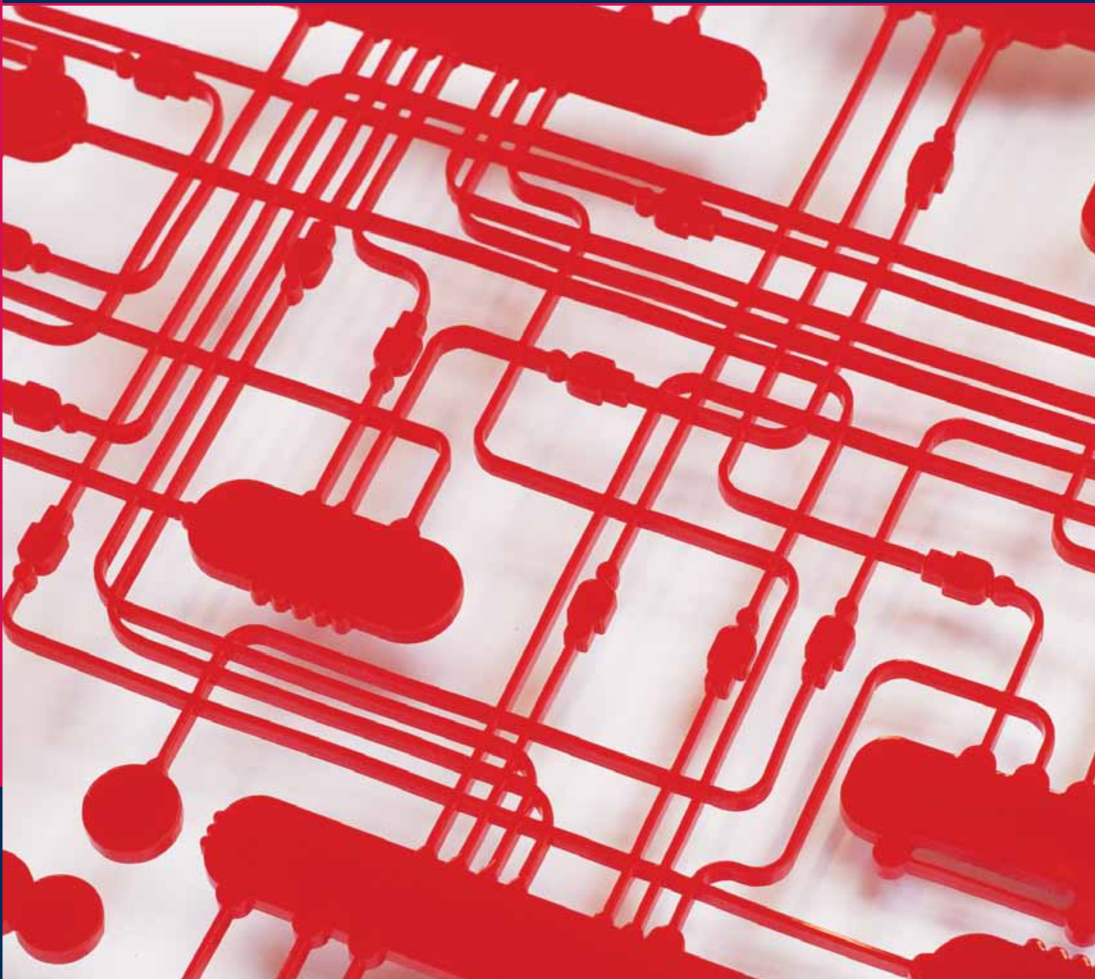
WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID



iOverheid

AMSTERDAM UNIVERSITY PRESS

iOverheid

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) werd in voorlopige vorm ingesteld in 1972. Bij wet van 30 juni 1976 (Stb. 413) is de positie van de raad definitief geregeld. De huidige zittingsperiode loopt tot 31 december 2012.

Ingevolge de wet heeft de raad tot taak ten behoeve van het regeringsbeleid wetenschappelijke informatie te verschaffen over ontwikkelingen die op langere termijn de samenleving kunnen beïnvloeden. De raad wordt geacht daarbij tijdig te wijzen op tegenstrijdigheden en te verwachten knelpunten en zich te richten op het formuleren van probleemstellingen ten aanzien van de grote beleidsvraagstukken, alsmede op het aangeven van beleidsalternatieven.

Volgens de wet stelt de WRR zijn eigen werkprogramma vast, na overleg met de minister-president die hiertoe de Raad van Ministers hoort.

De WRR is gevestigd:
Lange Vijverberg 4-5
Postbus 20004
2500 EA Den Haag
Telefoon 070-356 46 00
Telefax 070-356 46 85
E-mail info@wrr.nl
Website http://www.wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

iOverheid

Amsterdam University Press, Amsterdam 2011

Omslagafbeelding: Silo – Strategy. Concept. Design

Omslagontwerp: Studio Daniëls, Den Haag
Vormgeving binnenwerk: Het Steen Typografie, Maarssen

ISBN 978 90 8964 309 4
e-ISBN 978 90 4851 406 9
NUR 759 / 754

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Aan de Minister-President
Voorzitter van de Ministerraad
De heer drs. M. Rutte
Postbus 20001
2500 EA Den Haag

ons kenmerk
2011007/AK/am

direct nummer
070-356 4691

telefax
070-356 4685

onderwerp
WRR-rapportnr. 86
iOverheid

email
voorzitter@wrr.nl

datum
2 maart 2011

Het doet ons genoegen u hierbij het rapport *iOverheid* aan te bieden. De raad constateert dat de overheid als gevolg van de inzet van ICT *de facto* is veranderd in een informatie-Overheid. Bestuurlijk functioneert ze echter nog steeds als een eOverheid en dat brengt diverse problemen en kwetsbaarheden met zich mee. In het politiek-bestuurlijke denken en doen ligt de nadruk op losse technieken en individuele applicaties en niet op de genetwerkte informatiestromen die de bakens voor de overheid, en haar relatie met burgers, inmiddels stevig hebben verzet. Onder invloed van het uitwisselen van informatie in netwerken worden de grenzen tussen overheidsorganisaties, tussen beleidsterreinen en tussen publieke en private partijen diffuus. De hiermee gepaard gaande kwetsbaarheden, maar ook kansen, nopen tot een heroriëntatie. Voor de verdere digitalisering is het daarom van groot belang dat de overheid 'beseft een iOverheid te zijn' en haar bestuurlijke kaders en organisatie daarop aanpast. Hoewel het sturen op de verdere ontwikkeling van de iOverheid maar ten dele mogelijk is, laat de overheid nu veel kansen liggen om deze in goede banen te leiden.

Op basis van uitgebreid empirisch onderzoek, vele gesprekken in het veld en een uitgebreide bestudering van de literatuur presenteert de WRR allereerst een analyse van de ontwikkeling van de iOverheid. Daarnaast formuleert ze een agenda voor inhoudelijke en institutionele transformatie om het besef van de iOverheid op politiek en bestuurlijk niveau te verankeren en te laten aansluiten bij de ontstane situatie. Langs de gepresenteerde lijnen kan de overheid het pad van digitalisering met vertrouwen vervolgen. Tenslotte, voor zowel de inhoudelijke opdracht als de noodzakelijke institutionele transformatie, geldt dat de ontwikkeling van de iOverheid niet los gezien kan worden van het pad dat de bredere iSamenleving volgt. De raad gaat daarom kort in op de verantwoordelijkheid van de overheid in het licht van de ontwikkelingen in de huidige iSamenleving.

Ingevolge de Instellingswet ziet de raad graag de bevindingen van de ministerraad tegemoet.

De voorzitter,

Prof.dr. J.A. Knottnerus

De secretaris,

Dr. W. Asbeek Brusse

Lange Vijverberg 4-5, Postbus 20004, 2500 EA Den Haag
telefoon (070) 356 46 00, fax (070) 356 46 85, website: www.wrr.nl, e-mail: info@wrr.nl

INHOUDSOPGAVE

SAMENVATTING

De alomtegenwoordige inzet van informatie- en communicatietechnologie (ICT) door de overheid heeft ervoor gezorgd dat deze niet langer meer als een eOverheid, gericht op dienstverlening en gebruikmakend van techniek, kan worden gekarakteriseerd. In de dagelijkse praktijk is veeleer een iOverheid ontstaan, gekenmerkt door informatiestromen en -netwerken en gericht op niet alleen dienstverlening, maar ook controle en zorg. Deze iOverheid brengt vergaande veranderingen in de relatie tussen burgers en overheden met zich mee. Alhoewel deze iOverheid in de praktijk van beleid en uitvoering heel concreet is en daarmee reële gevolgen heeft, is ze nog nauwelijks op de politiek-bestuurlijke radar verschenen. Vanuit deze constatering bepleit dit rapport het verankeren van het besef 'een iOverheid te zijn' als een centrale opdracht en doet het een reeks inhoudelijke en institutionele aanbevelingen om de noodzakelijke paradigmawisseling van eOverheid naar iOverheid in goede banen te leiden.

Informatisering van samenleving en overheid

Informatisering is tot in de haarvaten van de overheid doorgedrongen en bepaalt in toenemende mate het reilen en zeilen van organisaties, de professionals die er werken en de relaties die zij met burgers onderhouden. De beleidsplannen voor de eOverheid – gericht op de (interne) bedrijfsvoering, de dienstverlening van de overheid en op de techniek zelf – ademen stuk voor stuk een groot vertrouwen in ICT als middel om de overheid effectiever, klantvriendelijker, toegankelijker, kwalitatief beter en voorbereid op de toekomst te maken. In toenemende mate wordt ICT enthousiast binnengehaald door beleid en politiek voor zowel de complexe administratieve opdracht van de overheid, als de aanpak van urgente maatschappelijke uitdagingen, zoals terrorisme, veiligheid, mobiliteit en goede en betaalbare zorg. Naast dienstverlening worden ook andere overheidstaken in snel tempo gedigitaliseerd.

De WRR constateert dat de inzet van technologie op zowel nationaal, lokaal als Europees niveau als welhaast vanzelfsprekend wordt gezien. Technologie wordt 'uitgerold', praktijken worden 'gestroomlijnd' en diensten 'geüpdatet'. Het 'technovertrouwen' van politiek en beleid vertaalt zich in grote ambities met ICT, niet alleen in technische, maar zeker ook in beleidsinhoudelijke zin. Huidige en populaire (beleids)doelen als 'maatwerk' en proactief beleid zijn ondenkbaar zonder deze achtergrond van digitalisering. Op gebieden als veiligheid en zorg worden systemen ingezet en gekoppeld om de toekomst in kaart te brengen en daarop alvast te anticiperen. Zo moet de Verwijsindex Risicojongeren 'een nieuw Maasmeisje' voorkomen, dienen Europese migratiedatabanken te garanderen dat zich geen nieuwe illegalen in Nederland vestigen en zijn opsporingsdatabanken en grensoverschrijdend uitgewisselde passagiers- en bankgegevens er om de wereld

te vrijwaren van een nieuwe terroristische aanslag. Plannen voor nieuwe systemen en de roep om meer en rijkere informatie ontstaan bovendien niet alleen in Den Haag. Op uitvoeringsniveau en binnen gemeenten groeit een wereld van verbonden systemen en informatieprocessen. En processen van globalisering zorgen ervoor dat het informatiebeleid van de Nederlandse overheid mede vorm krijgt in internationale en Europese applicaties en systemen. Ook op deze niveaus geldt een continue druk om de functies van de systemen uit te breiden, meer informatiecategorieën toe te voegen en om meer instanties toegang te verlenen tot de opgeslagen informatie.

Het politieke enthousiasme voor nieuwe applicaties en koppelingen van systemen en informatiestromen gaat hand in hand met argumenten als het vergroten van de veiligheid en verhogen van effectiviteit en efficiëntie. Deze waarden zorgen, gecombineerd met het probleemoplossende 'imago' van ICT, als het ware voor zichzelf: per maatregel (een systeem, een koppeling) blijken ze in de regel zwaarder te wegen dan waarden als transparantie, privacy, keuzevrijheid of *accountability*. Veel bestuurlijke 'eigenaren' of pleitbezorgers van applicaties hebben de neiging om ICT als een instrument te zien, en nemen aan – en dat wordt ook regelmatig uitgesproken – dat het primaire proces niet verandert. Daarmee wordt de onbedoelde doorwerking die digitalisering wel degelijk op het functioneren van de overheid heeft – alleen al omdat burgers veranderd zijn – niet of nauwelijks onderkend of waargenomen. Hoewel de instrumentele dimensie van ICT belangrijk is, leidt deze houding tot een zekere armoede, die zich met name in (gebrek aan) evaluaties toont. Geloofwaardige evaluaties zijn zeldzaam en missen goede maatstaven voor de beoordeling van applicaties. De discussie blijft steken in de veiligheid van de technologie (OV-chipkaart) of in financiële debacles (zoals de diverse mislukte ICT-projecten).

Het koppelen en uitwisselen van informatie gaat gepaard met de erosie van schotten tussen beleidsterreinen, tussen overheidsorganisaties en in relatie tot de private sector. Deze schotten worden in toenemende mate – ook in de publieke opinie – gezien als een sta-in-de-weg voor bestuurlijke daadkracht. De populariteit van gegevensuitwisseling binnen ketens en netwerken, gefaciliteerd door unieke nummers (Burgerservicenummer) en authentieke registraties, maakt dat informatie eenvoudig over traditionele grenzen heen vloeit – dit ondanks het feit dat de verantwoordelijkheid voor de kwaliteit en betrouwbaarheid daarvan niet zijn meegeëvolueerd. Informatie verspreidt zich en wordt door vele overheden gebruikt en bewerkt. Overheidsorganen met zeer verschillende taken en doelstellingen maken steeds vaker gebruik van dezelfde 'gepoolde' informatie. De verantwoordelijkheid voor (de juistheid van) informatie is echter niet scherp belegd waardoor burgers er rekening mee moeten houden dat 'hun' informatie in publieke en private handen een eigen leven kan gaan leiden.

Alle bovenstaande ontwikkelingen worden in het politieke debat gepropageerd, bediscussieerd en beoordeeld vanuit een scala aan motieven, ideeën en normatieve oriëntaties. De meest bekende daarvan zijn efficiëntie, effectiviteit, veiligheid, privacy en transparantie. De uiteindelijke vorm die een nieuw systeem of een nieuwe koppeling van informatiebronnen krijgt, is de uitkomst van een complexe dynamiek tussen al deze maatstaven. Die uitkomst betreft niet alleen de technologie – vaak de focus van het debat –, maar vooral ook de sociale, bestuurlijke en juridische uitwerking die veel minder aan bod komt. Om enerzijds meer helderheid binnen deze dynamiek aan te brengen en anderzijds handvatten te bieden voor de noodzakelijke afwegingen die tussen de motieven gemaakt dienen te worden, brengt de WRR ze onder in drie betekenisclusters: stuwende beginselen (zoals veiligheid, effectiviteit en efficiëntie), verankerende beginselen (privacy en keuzevrijheid) en procesmatige beginselen (transparantie en accountability). Stuwende beginselen zijn verbonden met de *drive* van de overheid om ICT in tal van domeinen in te zetten en staan in het teken van verbetering en kwaliteitswinst. Verankerende beginselen staan voor het waarborgen van vrijheden, het in kaart brengen van 'stille verliezen' bij voortgaande digitalisering en voor het vrijwaren van de autonomie van het individu. Ze vormen als het ware een tegenwicht voor de stuwende beginselen. Procesmatige beginselen ten slotte staan voor de procedurele omlijsting die het mogelijk maakt dat afweging tussen de stuwende en verankerende beginselen met name inzichtelijk en toetsbaar is.

iOverheid als realiteit

Dit rapport laat zien dat de overheid stapje voor stapje, besluit na besluit, onder invloed van digitalisering fundamenteel van karakter verandert. De facto en bijna ongemerkt heeft zich een praktijk ontwikkeld, waarin samenhangende informatiestromen het karakter van de overheid domineren. En daarmee bepalen deze informatiestromen de nieuwe mogelijkheden, maar ook de afhankelijkheden en de kwetsbaarheden voor zowel de overheid als haar burgers. In de dagelijkse werkelijkheid van politiek en bestuur wordt echter allesbehalve vanuit het samenhangende idee van deze informatie-Overheid – *iOverheid* – gedacht en gewerkt: het overgrote deel van de overheidsinitiatieven voor digitalisering en de informatiestromen die daaruit volgen, worden geïsoleerd bepleit, beoordeeld en ingevoerd. Individuele initiatieven worden niet of nauwelijks beoordeeld op hun (potentiële) invloed op de overheid en de samenleving als geheel. De belangrijkste omissie daarbij is dat ze niet of nauwelijks worden bezien vanuit het perspectief van de snelgroeiende en vertakkende informatiestromen. De iOverheid staat niet op het netvlies van politiek en beleid en dat is gezien de gestaag verdergaande informatisering problematisch.

De opeenstapeling van ad-hocbesluiten over nieuwe technieken, het ontbreken van een besef van het ontstaan van een iOverheid en het gebrek aan debat daarover, maken dat de iOverheid zich als het ware onbegrensd en daarmee ook 'gren-

zeloos' ontwikkelt. De grenzen aan de uitwaaiering van individuele applicaties en de verknoping van informatiestromen zijn niet gegeven, omdat niemand zich hoeder voelt van het geheel. Informatieverzameling en koppelingen lijken nauwelijks meer in te kaderen. Het resultaat is dat informatie vervuilt, onduidelijk is wie verantwoordelijk is voor informatiestromen en dat burgers, bedrijven en ook instanties binnen de overheid zelf, verst(r)ikt raken in de datakluwen van de overheid. Vragen en afwegingen op het niveau van de samenhang van informatiestromen en de gevolgen daarvan blijven liggen. Dat maakt niet alleen burgers, maar zeer zeker ook de overheid zelf kwetsbaar. Het bredere perspectief van de iOverheid en een zorgvuldige en toetsbare afweging tussen de stuwende, verankerende en procesmatige beginselen ontbreekt in het Nederlandse politiek-bestuurlijke debat. Alhoewel de iOverheid feitelijk nog sterk in opbouw en ontwikkeling is, en begripsmatig nog nauwelijks op de radar is verschenen, heeft ze wel degelijk al reële gevolgen. Tegelijkertijd worden deze gevolgen vanwege het gebrekkige 'bewustzijn' van de karakteristieken van de iOverheid nauwelijks in de beleidsontwikkeling betrokken en ontbreekt het aan een goed politiek-bestuurlijk besef van *wat* zich ontwikkelt, laat staan van een besef *hoe* die ontwikkeling in goede banen is te leiden. Wil de Nederlandse overheid de verdere digitalisering in zorgvuldige banen leiden waarbij er tegelijkertijd ruimte is voor innovatie met behulp van ICT, dan zal ze in woord en daad de transformatie van een eOverheid naar een iOverheid dienen te maken. De centrale opdracht voor de overheid, of eigenlijk voor alle lagen van de overheid, is om te beseffen dat ze een iOverheid is geworden, met alle consequenties van dien. Deze opgave vereist een inhoudelijk andere oriëntatie, gecombineerd met de ontwikkeling van een bijbehorend institutioneel kader. Daarbij is het van groot belang dat afscheid wordt genomen van de nauwe blik op individuele applicaties en dat de aandacht zich verlegt naar de vernetwerkte informatiehuishouding van de overheid. Tot slot vergt de vormgeving van iOverheid een open houding naar de ontwikkelingen binnen de informatiesamenleving (iSamenleving). De iOverheid kan niet eigenstandig en in een isolement worden vormgegeven, en dus moet zij het credo 'Betrek de iSamenleving bij de duurzame uitbouw van de iOverheid' volgen.

Bestuurlijke uitgangspunten voor de iOverheid

Bij de inhoudelijke opdracht voor de bestuurlijke transformatie naar een iOverheid zijn twee zaken van wezenlijk belang. Een zorgvuldige ontwikkeling van de iOverheid kan allereerst niet zonder een open afweging tussen de stuwende, verankerende en de procesmatige beginselen. Hiernaast geldt dat van de overheid bij zowel deze afweging als de verdere inrichting van beleid en uitvoering extra behoedzaamheid verlangd mag worden wanneer sprake is van een drietal in dit rapport gesignaleerde processen van informatieverwerking. Deze processen – die in symbolische zin zijn voorzien van waarschuwingsvlaggen – houden verband met a) het vernetwerken van informatie, b) het samenstellen en verrijken van informatie en c) het voeren van preventief beleid op basis van informatie.

De drie in dit rapport gehanteerde clusters van beginselen – stuwend, verankerend en procesmatig – moeten op alle niveaus waar beslissingen worden genomen met elkaar in balans worden gebracht. Dit is geen geringe opgave, aangezien een kwantitatief getint concept als efficiëntie en een meer normatief concept als keuzevrijheid of een procesmatig concept als accountability, duidelijk in verschillende registers van analyse thuishoren. Toch vereist een evenwichtige ontwikkeling van de iOverheid een doordachte afweging tussen deze clusters van beginselen, waarbij ze geëxpliciteerd, toetsbaar en publiekelijk verantwoord moeten worden. Dat is nu te weinig het geval. De overheid moet haar eigen afwegingen zo expliciet mogelijk wereldkundig maken en wel op alle niveaus: van de voorbereiding en introductie van een concrete toepassing tot aan de omvattende vertakking van processen en informatiestromen waaruit de iOverheid is opgebouwd. Dat geldt niet alleen voor het nationale niveau, maar ook voor de afwegingen die op het internationale, en met name op het Europese niveau worden gemaakt. Het expliciet en zoveel mogelijk toetsbaar maken van de beginselen zou een aantal zaken laten uitkomen en openlijk bespreekbaar maken. Bijvoorbeeld dat vaak sprake is van ongefundeerd politiek-bestuurlijk optimisme ten aanzien van de mogelijkheden van ICT, hetgeen de onderliggende reden is voor onhaalbare deadlines en kostbare ICT-mislukkingen. Explicitering zou ook duidelijk maken dat s*pill over* en *function creep* vaak stilletjes zijn ingecalculeerd. Het werkelijke besef 'een iOverheid te zijn' vereist dat de politiek de uitdrukking 'regeren is vooruitzien' ook serieus neemt in het digitale domein en toepast op de impliciete, maar voorzienbare toekomstige ontwikkelingen van informatisering. De overheid neemt in haar beleid vaker een voorschot op de toekomst en het zou haar sieren om dat in de politieke afweging ook, en met een open vizier, te doen.

De inhoudelijke opgave vereist ten tweede dat de overheid bij de verdere informatisering een aantal kenmerken van informatie veel bewuster dan nu het geval is in acht neemt. Daarbij gaat het om *processen* van informatieverwerking en -gebruik, juist omdat die processen van grote invloed zijn op het karakter en de betrouwbaarheid van de informatie waarop de iOverheid draait. Aan drie, onderling gerelateerde, processen worden daarom waarschuwingsvlaggen meegeven: wanneer informatie onderdeel dan wel resultaat is van deze processen dient de overheid alert te zijn op de kwaliteit van de informatie en op de vraag wie de verantwoordelijkheid voor de informatie draagt. De drie ontwikkelingen die deze drie vlaggen dragen zijn de volgende.

1 Het *vernetwerken* van informatie, i.e. het gezamenlijk gebruik en beheer van informatie in een netwerk van actoren.
2 Het *samenstellen en verrijken* van informatie, i.e. het creëren van nieuwe informatie en profielen op basis van verschillende bronnen uit verschillende contexten.
3 Het voeren van *preventief* en proactief beleid op basis van informatie, i.e. het

actief beoordelen van en ingrijpen in de samenleving op basis van informatiegestuurde risicocalculatie.

Deze drie informatieprocessen vormen de kern van de iOverheid en stellen haar in staat om beleid te verfijnen, op maat te snijden, een omvattend beeld te verkrijgen van burgers en beleidsproblemen en daar waar nodig proactief op te handelen. Tegelijkertijd zijn het ontwikkelingen die van invloed zijn op informatie zelf: op het karakter, de betrouwbaarheid, de kenbaarheid, de contextualiteit en herleidbaarheid van informatie. Veel meer dan nu het geval is dient het besef door te dringen dat het juist deze drie ontwikkelingen zijn die grote gevolgen hebben voor (a) de *inhoudelijke* kwaliteit van informatie en (b) voor de eisen aan de *organisatorische* inbedding van informatiestromen. Voortdurende rijksbrede en proactieve aandacht voor de kwaliteit en kwetsbaarheid van informatie en informatieprocessen is daarom van groot belang. Ook is een veel grotere mate van openheid en transparantie richting burgers noodzakelijk om hen inzicht te bieden in de informatie die over hen is vergaard en hen tevens te faciliteren de informatie waar nodig te corrigeren. Burgers staan nu vrijwel machteloos als zij persoonlijk worden geconfronteerd met fouten in de uitgestrekte informatienetwerken van de iOverheid die soms grote gevolgen hebben. Ten slotte vraagt het 'geheugen' van de iOverheid expliciete aandacht. Zowel het belang van 'vergeten' – mensen moeten niet voor eeuwig afgemeten worden aan de informatie die de overheid over ze heeft opgeslagen – als dat van bewaren en archiveren verlangt een radicale cultuuromslag en een verankerde strategie.

Grenzen aan de groei van de iOverheid

Een onbewuste iOverheid zal de natuurlijke neiging hebben om verder te groeien: 'grenzen aan de groei' komen pas met bewustzijn in zicht. Een zorgvuldige inrichting en ontwikkeling van de iOverheid vereist dus ook het durven stellen van grenzen aan die overheid. Hoewel dit rapport die grenzen niet markeert – die zijn in essentie politiek – geeft het wel aan welke grensgebieden overwogen moeten worden. Allereerst dwingt de combinatie van een expliciete afweging van beginselen en het in acht nemen van de waarschuwingsvlaggen tot nadenken over de grenzen van de iOverheid. Ook de vermenging tussen service, *care* en *control* en de diffuse grenzen tussen publieke en private informatiestromen kunnen aanleiding zijn tot het stellen van grenzen. Van groot belang is ook de constatering dat het internet een totaal andere informatieomgeving heeft gecreëerd waaraan ook de iOverheid zich niet kan onttrekken en waarbinnen ze heeft te functioneren. Ook in relatie tot deze 'buitenwereld' kunnen beredeneerde begrenzingen van groot belang zijn.

Een institutionele agenda voor de transformatie naar een iOverheid

Gericht werken aan een zorgvuldige uitbouw van de iOverheid vraagt niet alleen in inhoudelijke zin, maar ook op institutioneel niveau om de nodige aanpassingen.

Een overheid die op digitaal vlak van gedaante is veranderd heeft zich ook in organisatorisch opzicht aan te passen. Een op informatieniveau verknoopte overheid verlangt een verantwoordelijkheidsstructuur die past bij de nieuwe realiteit en is voorzien van de nodige slagkracht. Het besef 'een iOverheid te zijn' is geen rustig bezit, maar een permanente opgave die uiteindelijk in alle lagen van de overheid moet worden verankerd. Op de korte termijn zal dat besef echter centraal moeten worden aangejaagd. Om de doelen voor de iOverheid handen en voeten te geven is daarom een institutionele transformatie nodig die drie functies bij de overheid belegt en verankert.

1 De *strategische functie*, i.e. het waarborgen van een weloverwogen verdere ontwikkeling van de iOverheid.
2 De *maatschappelijke functie*, i.e. het versterken van de transparantie van de iOverheid voor burgers en het versterken van de accountability van de iOverheid ten opzichte van burgers die in informatienetwerken verstrikt raken.
3 De *operationele functie*, i.e. het verbeteren van de weloverwogen aansluiting tussen beleid, uitvoering, technologie, informatiestromen en netwerken. Het verbeteren van het opdrachtgeverschap van de overheid.

Deze drie functies vormen de absolute ondergrens van wat nodig is om het besef van de iOverheid vorm te geven en te handelen naar de consequenties die de nieuwe realiteit met zich meebrengt. Het is niet eenvoudig om de bij deze drie functies behorende instituties goed vorm te geven, maar het is wel zaak deze functies daadwerkelijk aan organisaties toe te vertrouwen. De institutionele transformatie als zodanig is echter vele malen belangrijker dan de in dit rapport voorgestelde (naambordjes van) instituties. Op het strategische niveau is dat een permanente commissie voor de iOverheid die processen van digitalisering beschouwt en beoordeelt in het licht van de iOverheid als geheel en die aan het parlement rapporteert. Op het niveau van de maatschappelijke functie is dat de oprichting van een iPlatform om de transparantie van de iOverheid ten opzichte van burgers te centraliseren en vergroten. De accountability kan vorm en inhoud krijgen via een iAutoriteit die verantwoordelijk is voor de afhandeling (met doorzettingsmacht) van problemen die burgers ondervinden met de iOverheid. Op het operationele niveau ten slotte is het van groot belang het opdrachtgeverschap te professionaliseren en kennis op het snijvlak van techniek en beleid te prioriteren in plaats van kennis van de techniek zelf.

In de kern gaat dit rapport over de verantwoordelijkheid van de overheid voor haar eigen gebruik van ICT. Maar de overheid heeft uiteraard ook een rol te spelen in de informatiesamenleving. Behalve de verantwoordelijkheid voor de iOverheid berust bij de overheid ten principale ook een zekere verantwoordelijkheid voor het functioneren van de iSamenleving. Wat dient de overheid zich in de ontwikkeling van de informatiesamenleving aan te trekken en (hoe) heeft zij daarin te interveniëren? Burgers en bedrijven worden voortgestuwd door enthousiasme voor

nieuwe technische mogelijkheden en overwegingen van winstgevendheid. Waar deze structureel onvoldoende worden afgewogen tegen verankerende beginselen en onvoldoende in balans worden gebracht met een uitwerking van procesmatige beginselen die informatiestromen voor burgers transparant en, indien nodig, bekritiseerbaar maken, dient de iOverheid zich in ieder geval af te vragen of ze aan zet is.

TEN GELEIDE

In dit rapport schetst de WRR zijn visie op de digitalisering van de overheid. Het rapport is opgesteld door een projectgroep onder leiding van prof.mr. Corien Prins, lid van de raad. De projectgroep bestond verder uit de volgende stafleden: dr. Dennis Broeders (projectcoördinator), dr. Colette Cuijpers, mr. Henk Griffioen, drs. Anne-Greet Keizer en Esther Keymolen MA. In eerdere fases hebben mr.ir. Mark van Loon, dr.ir. Annemarth Idenburg, Tamara Snijders MSc en dr. Astrid Souren een bijdrage aan de werkzaamheden geleverd.

Dit rapport is tot stand gekomen op basis van een uitvoerige analyse van de rijke (internationale) wetenschappelijke literatuur, onderzoek dat in opdracht van de WRR is verricht, bijeenkomsten en vele gesprekken met externe deskundigen uit diverse lagen van het bestuur, de politiek en de wetenschap. Voor een deel waren deze deskundigen verbonden aan ministeries, colleges (Nationale Ombudsman, College Bescherming Persoonsgegevens, Algemene Rekenkamer, Raad van State), parlement (leden van de Eerste en Tweede Kamer), uitvoeringsinstanties, kennisinstituten (Rathenau Instituut, HEC), Nederlandse universiteiten, bedrijven en andere relevante instellingen (ECP-EPN, ICTU, BPR, enz.) voor een deel aan buitenlandse universiteiten, Europese instituties (Europese Commissie, Europees Parlement en EDPS) en de Nederlandse Permanente Vertegenwoordiging te Brussel. Als bijlage bij dit rapport treft de lezer een lijst aan van personen met wie in het kader van dit rapport of een van de voorstudies is gesproken. De raad is al deze personen zeer erkentelijk voor hun tijd, kennis en suggesties, die van onschatbare waarde zijn geweest. Het ondersteunende onderzoek dat in opdracht van de WRR voor dit rapport is verricht is in twee vormen gepubliceerd. Een deel van de studies is als hoofdstuk opgenomen in de tegelijkertijd met dit rapport gepubliceerde achtergrondstudie *De staat van informatie* (Broeders, Cuijpers & Prins 2011). Een ander deel van de studies is vanaf het najaar van 2010 verschenen als webpublicatie via de website van de WRR, in de serie iOverheid. Al deze publicaties kunnen via www.wrr.nl worden gedownload. De raad is alle auteurs en deskundigen erkentelijk voor hun bijdrage en participatie in de werkconferenties die in het kader van deze voorstudies zijn gehouden. De boodschap van dit rapport wordt op alternatieve wijze op de site www.ioverheid.nu gepresenteerd.

Tijdens een door de WRR en het Oxford Internet Institute (OII) georganiseerd besloten seminar in mei 2010 heeft de projectgroep met een internationaal gezelschap van wetenschappers in Oxford uitvoerig gedebatteerd over de voorlopige uitkomsten en aanbevelingen van het project. De raad dankt alle aanwezigen voor hun bijdrage aan die discussie. Tot slot geldt een bijzonder woord van dank aan enkele mensen die in de laatste fase actief commentaar leverden op de conceptrapportage dan wel bij aanvang meedachten over de opzet van het project:

dr. K. van Beek, mr. A. van Bellen, mr. A. Brenninkmeijer, prof.mr. Y. Buruma, prof.dr. W.B.H.J. van de Donk, drs. M. Hillenaar, prof.dr. I.Th.M. Snellen, prof.dr. S. Zouridis, prof.dr. A. Zuurmond.

DEEL I

INLEIDING EN ONDERZOEKSKADER

1 DE DIGITALISERING VAN BURGERS EN OVERHEID

1.1 DE EXISTENTIËLE ROL VAN DIGITALISERING

Digitalisering is een fascinerend fenomeen waarvan de invloed op onze samenleving nauwelijks te overschatten valt. Tal van vitale maatschappelijke en economische processen zijn inmiddels grotendeels afhankelijk van (goed functionerende) ICT-systemen die in essentie werken op basis van eindeloze reeksen getallen nul en één. Simpele cijfers die in staat zijn de variëteit van tekst-, beeld- of geluidssignalen uit de analoge wereld in een digitale variant om te zetten. Kenmerkend voor deze digitaliseringsslag is de relatieve eenvoud waarmee informatie verzameld, opgeslagen, doorzocht en gedeeld kan worden. Het levert onze samenleving een ongekende rijkdom aan nieuwe producten, diensten en applicaties op. En dat alles in een adembenemend tempo. Met een druk op de knop wordt informatie op het internet gedeeld via toepassingen als Twitter, blogs, websites of Hyves. Bedrijven, overheden en non-profitorganisaties vullen, al dan niet online, databases met gegevens over de meest uiteenlopende onderwerpen: van koopgedrag tot wanbetalers, van DNA-gegevens tot de vingerafdrukken van de hele Nederlandse bevolking. Digitale informatie ontwikkelt zich tot een universele taal die de wereld een stuk kleiner maakt dan ze was. De eenvoudige repliceerbaarheid van informatie leidt zelfs tot mondiale schokgolven, zoals de WikiLeaks-affaire – wel beschreven als "the first sustained confrontation between the established order and the culture of the internet" (Naughton 2010b) – van eind 2010 illustreert.

De effecten van digitalisering (ook wel informatisering genoemd) zijn groot maar ook zeer divers. Waar WikiLeaks de ontwrichtende potentie belichaamt (of men die nu positief of negatief beoordeelt), is de invloed in meer 'traditionele' contexten zoals het functioneren van overheden zelf ook massief. Het is niet verwonderlijk dat de publieke sector eveneens enthousiast de vruchten van het fenomeen digitalisering plukt. Binnen het brede domein van de overheid is de afgelopen jaren een indrukwekkend arsenaal aan initiatieven ontplooid. Deze richten zich zowel op een verbetering van de dienstverlening aan de burger als op het optimaliseren van de samenwerking tussen ambtenaren en diensten in de backoffice van de overheid. De veranderingen op het vlak van de dienstverlening springen bij het publiek veelal het meest in het oog. Wie gebruik wil maken van publieke voorzieningen kan nu vaak ook de digitale route bewandelen. Uittreksels, vergunningen en andere bescheiden zijn via de website van vrijwel elke gemeente aan te vragen. Soms is het digitale loket zelfs de enige weg. Ondernemers zijn bijvoorbeeld verplicht om een groot aantal aangiften bij de Belastingdienst elektronisch in te dienen. Voor burgers wordt hard gewerkt aan het overheidsportaal mijn.overheid.nl, alwaar ze met behulp van hun DigiD kunnen inloggen om zo rechtstreeks met de overheid zaken te doen.

Box 1.1 Alledaagse digitalisering voor burgers

Christine drukt op ‘verzenden’. Met behulp van haar DigiD heeft ze via de pc zojuist een vergunning aangevraagd voor het buurtfeest dat ze met het buurtcomité binnenkort in de straat wil organiseren. De digitale aanvraag spaart haar weer een gang naar de deelgemeente uit. Nu ze toch online is en haar DigiD-inlogcode bij de hand heeft, maakt ze meteen van de gelegenheid gebruik om haar aanvraag huur- en zorgtoeslag aan te passen. Ze is namelijk meer gaan werken, waardoor haar inkomsten zijn gewijzigd. Via het softwareprogramma dat ze heeft gedownload van de website van de Belastingdienst gaat ze aan de slag. Gegevens die bij de Belastingdienst bekend zijn, staan al voor haar ingevuld. Dat is wel zo gemakkelijk. Wanneer ook dit klusje is geklaard, komt de binnengekomen post aan de beurt. Een brief van de Dienst Uitvoering Onderwijs met de melding dat ze op basis van de bij de Belastingdienst bekende gegevens over 2009 de draagkrachtmeting van Christine hebben berekend. Als de gegevens in deze brief kloppen, hoeft ze niks te ondernemen en krijgt ze binnenkort te horen welk aangepast bedrag ze maandelijks aan studieschuld terug moet betalen. Een andere brief is van Stadsregionaal Instrument Sluitende Aanpak (SISA), een digitaal informatienetwerk van jeugdhulporganisaties. In de brief staat dat haar zoon Martin door twee verschillende instanties – zijn school en jeugdwerk – is gemeld in het SISA-signaleringssysteem. Dit systeem houdt bij welke instanties contact houden met een jeugdige die mogelijk risico loopt in zijn of haar ontwikkeling. Christine maakt zich ongerust en vraagt zich af wat er met Martin aan de hand is. Ze leest nog een keer aandachtig de brief en bijgevoegde brochure, terwijl ze internet opstart. Even googlen wat SISA allemaal inhoudt…

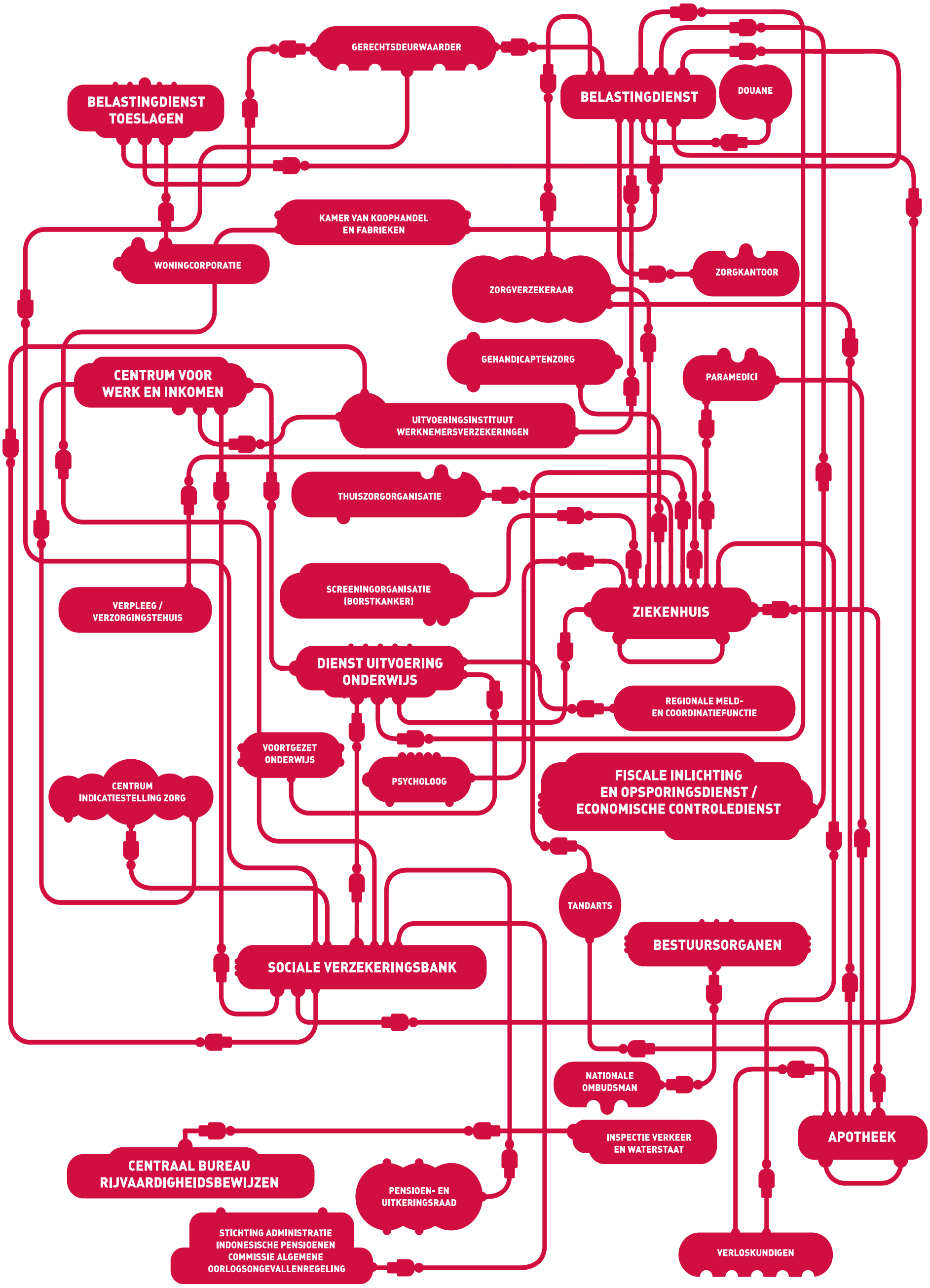
Maar op andere terreinen dan dienstverlening waar de overheid een bepaalde verantwoordelijkheid draagt, zoals zorg, veiligheid en sociale zekerheid, groeit de invloed van ICT-applicaties evenzeer. Zo is er voor burgers die een uitkering aanvragen het Digitaal Klantdossier. Via dit dossier kunnen verschillende ketenpartners zoals de gemeente, de Sociale Verzekeringsbank (SVB) en het Uitvoeringsinstituut Werknemersverzekeringen (UWV) informatie delen en hoeft de burger maar één keer gegevens aan te leveren. Om onder meer missers te voorkomen en vroegtijdig in te kunnen grijpen bij risico’s wordt in het brede domein van de zorg gewerkt aan het Elektronisch Patiëntendossier (EPD), het Elektronisch Kinddossier (EKD) en aan de Verwijsindex Risicojongeren (VIR). In het kader van de veiligheid en handhaving voert men *body scans* uit op Schiphol, maakt men gebruik van camera’s boven de snelweg en onderzoekt het Kennis- en expertisecentrum voor intelligente data-analyse (Kecida), een afdeling van het Nederlands Forensisch Instituut, allerhande informatiestromen (op bijvoorbeeld internet) om onder meer de politie te ondersteunen bij handhaving en opsporing. Tegelijkertijd toont de Amsterdamse zedenzaak van december 2010 dat er bij de grensoverschrijdende gegevensuitwisseling (in dit geval over het feit dat de hoofdverdachte eerder in Duitsland was veroordeeld voor bezit van kinderpornografie) nog een wereld te winnen valt. Desalniettemin, de inzet van digitale applicaties op terrei-

nen als dienstverlening, zorg en veiligheid moet ervoor zorgen dat de overheid zich beter van haar taken kan kwijten en de burger sneller van dienst kan zijn. Voor de burger zelf betekent dit onder meer dat hij of zij veel makkelijker toegang tot de overheid heeft, maar tegelijkertijd in toenemende mate door de overheid geregistreerd wordt en voor die overheid bekend is. In het digitale tijdperk is de gemiddelde burger vaak veel bekender voor de overheid dan hij of zij zal beseffen.

Digitalisering beperkt zich niet tot de zichtbare interacties tussen burgers en overheden. Achter de voordeur van de overheid wordt ICT breed ingezet om werkprocessen te stroomlijnen en samenwerking tussen organisaties mogelijk te maken. De veranderingen die dit 'achter de schermen' met zich meebrengt zijn weliswaar minder zichtbaar voor het grote publiek dan projecten zoals het EPD of de inzet van body scans op Schiphol die in de media uitvoerig worden besproken, maar daarom niet minder belangrijk. Een gestroomlijnde informatiehuishouding is immers een noodzakelijke voorwaarde voor een optimaal presterende overheid. In dit kader faciliteert bijvoorbeeld het Routerings Instituut (inter)Nationale Informatiestromen (RINIS) een veilige en geautomatiseerde berichtenuitwisseling tussen verschillende publieke instanties. Als een soort digitale postbode zorgt RINIS ervoor dat gegevens op het juiste adres terechtkomen, zonder de inhoud van het bericht te kennen. Bovendien kunnen aangesloten partners via RINIS ook toegang krijgen tot de authentieke basisregistraties, zoals de Gemeentelijke Basisadministratie (GBA), een ander belangrijk onderdeel van de informatiehuishouding van de overheid. De basisregistraties vormen eigenlijk een data-set bestaande uit de meest gevraagde en gebruikte gegevens zoals adressen, persoonsgegevens, bedrijfsnamen en locatiegegevens. Het doel hiervan is dat overheden in hun taakuitvoering gebruik kunnen maken van dezelfde essentiële en betrouwbare gegevens uit de basisregistraties. Een ander voorbeeld is het Burgerservicenummer (BSN) dat als 'sleutel' fungeert voor het uitwisselen van persoonsgerelateerde gegevens. Het gebruik van het BSN moet het uitwisselen van persoonsgerelateerde gegevens eenvoudiger en betrouwbaarder maken. Het delen van gegevens over burgers, het elkaar onderling inzage geven in informatiesystemen of het koppelen van systemen is kortom aan de orde van de dag. Het onderstaande overzicht (figuur 1.1) ontleend aan de website burgerservicenummer.nl geeft een eerste indruk.

De hierboven aangestipte ontwikkelingen zijn maar een fractie van wat er op het vlak van digitalisering bij de overheid plaatsvindt. Wie wordt gevraagd een actueel overzicht van al deze initiatieven te schetsen, heeft een welhaast onmogelijke opdracht. En dat is niet alleen vanwege de enorme hoeveelheid projecten, de verspreiding daarvan over alle hoeken en gaten van de publieke sector en de diffuse grenzen bij veel van deze projecten met de private sector. Het beeld is ook onmogelijk vast te leggen vanwege de sterke dynamiek en verandering. Onder invloed van nieuwe technologische mogelijkheden, politiek-bestuurlijke ambities en wensen en verwachtingen in de samenleving wijzigt het overzicht vrijwel constant.

Figuur 1.1 **Gegevensstromen tussen (overheids)instanties gefaciliteerd door BSN**



Bron: www.burgerservicenummer.nl

Daarbij komt dat de initiatieven lang niet altijd tot de grenzen van ons land beperkt blijven, dan wel puur een aangelegenheid van de Nederlandse overheid zijn: ook hier spelen europeanisering en internationalisering prominente rollen. Maar één beeld is in ieder geval wel te schetsen: digitalisering is tot in de haarvaten van de overheid doorgedrongen en bepaalt in belangrijke en toenemende mate het reilen en zeilen van organisaties, de professionals die er werken en de relaties die zij met burgers onderhouden.

Nu digitale toepassingen een vaste plaats in ons dagelijks bestaan hebben veroverd en hun alomtegenwoordigheid verder groeit, tekenen zich de meer fundamentele veranderingen en consequenties voor de samenleving en overheidsinstituties af. Zowel de burgers en bedrijven als de overheid herijken hun positie in een maatschappij die steeds meer de vorm aanneemt van een informatiesamenleving (zie par. 1.2). Deze informatiesamenleving heeft in essentie een netwerkkarakter, waardoor de rollen en posities van overheden en burgers veranderen en verschuiven. Meer en meer wordt duidelijk dat deze verandering niet alleen consequenties heeft voor het informatiegebruik door burgers en overheden, maar eveneens van betekenis is of zou moeten zijn voor de bestuurlijke inrichting en verantwoordelijkheidsverdeling. Van diverse zijden is er dan ook op gewezen dat digitalisering noodzaakt tot een transformatie van de inrichting van het openbaar bestuur (Frissen 1996; Eenmalige Adviescommissie ICT en Overheid 2001; Bekkers, Lips & Zuurmond 2005: 746). Welke richting bij deze transformatie moet worden ingeslagen is echter een allesbehalve eenvoudige vraag. Digitalisering brengt naast de grote kansen namelijk ook, voor zowel burgers als de overheid zelf, tal van nieuwe risico's en kwetsbaarheden met zich mee, die bovendien niet altijd even zichtbaar zijn.

Zo mag het digitaal delen van informatie dan tijd- en kostenbesparend zijn, wanneer foutieve gegevens worden uitgewisseld, blijkt het zeer moeilijk om al die verknoopte informatiestromen en bestanden op te schonen, met alle gevolgen van dien voor de betrokken burger. Uit een onderzoek van de gemeente Amsterdam bleek enkele jaren geleden dat maar liefst in 7,3 procent van de adresgegevens in de Gemeentelijke Basisadministratie (GBA) fouten voorkomen (Adviescommissie Informatiestromen Veiligheid 2007: 27). Het is hierbij niet duidelijk of het fraude of 'slechts' fouten betreft. Wanneer het wel duidelijk om fraude gaat, zoals bij de zaak rondom R. Kowsoleea die slachtoffer werd van identiteitsfraude, blijkt het terugdraaien van fouten in informatiestromen ontzettend moeilijk. Een misdadiger die opereerde onder de naam van Kowsoleea maakte dat de man abusievelijk in tal van politie- en andere overheidsdatabases als crimineel te boek kwam te staan. Dit leidde tot invallen in zijn huis, aanhoudingen op Schiphol en tal van dagvaardingen. Ondanks verwoede pogingen om zijn naam gezuiverd te krijgen, ondervindt hij nog steeds last van deze identiteitsdiefstal. Bij zulke kafkaëske toestanden dringt de vraag zich op wie er verantwoordelijk is voor de juistheid van gegevens in een netwerk van informatiestromen. Als het gaat om de politiebestan-

den waar Kowsoleea zoveel hinder van ondervond, blijkt er in ieder geval geen overkoepelend aanspreekpunt te bestaan.

In z'n algemeenheid lijken burgers niet of nauwelijks stil te staan bij de nieuwe, veelal negatievere, bewijspositie waarin ze terechtkomen wanneer ze al dan niet verplicht overstappen op de digitale diensten. Bovendien blijken nieuwe informatiesystemen als het Elektronisch Kinddossier (EKD) en de Verwijsindex Risicojongeren (VIR) geen neutrale digitaliseringslagen die uitsluitend de efficiëntie van bestaand beleid verhogen of de veiligheid vergroten. Ze zijn tegelijkertijd van invloed op de aard van de relatie die burgers en professionals met elkaar onderhouden en zetten principes als privacy en keuzevrijheid, van zowel burger als professional, in een ander licht en soms onder druk. De Staatscommissie Grondwet constateerde dat de overheid bij de uitvoering van publieke taken in toenemende mate een elektronische overheid is geworden (Staatscommissie Grondwet 2010: 67). En alhoewel de Staatscommissie verdeeld is over de noodzakelijke wijzigingen van de Grondwet in het licht van digitalisering, is de richting van de aanbevelingen onmiskenbaar: er is alle reden de grondwetgever aan het werk te zetten met het oog op de veranderde digitale samenleving. In het digitale tijdperk neemt de betekenis van informatie(grond)rechten toe, aldus de Staatscommissie, wat reden is de normativiteit van de Grondwet te versterken en de betekenis ervan voor de burger te vergroten (Staatscommissie Grondwet 2010: 69).

Digitalisering raakt ook de positie van de overheid. Ze wordt afhankelijk van systemen en daarmee ook kwetsbaar voor het haperen of zelfs de uitval ervan, of die nu veroorzaakt wordt door virussen, *cybercrime*, gebrekkig onderhoud, vervuilde en verouderde bestanden of zelfs de onkunde van gebruikers. "Zonder de ICT-voorzieningen kunnen we niets meer, zo kwetsbaar en zo afhankelijk zijn we inmiddels allemaal geworden", aldus minister Opstelten tijdens het Veiligheidscongres op 11 november 2010. Maar de afhankelijkheid toont zich ook op een ander vlak: de digitale overheid leunt zwaar op de kennis en invloed van externe consultants, ontwikkelaars en leveranciers die systemen ontwerpen, implementeren en onderhouden.

ICT-initiatieven brengen kortom nieuwe kansen, kwetsbaarheden en risico's aan het licht die de richting en inrichting van de informatiesamenleving bepalen. Die kansen en risico's vormen de aanleiding voor dit rapport. Als overheidsinstellingen het onderlinge informatieverkeer 'stroomlijnen' en 'keteninformatisering' en informatienetwerken enthousiast omarmen, welke gevolgen heeft dat dan voor de inrichtingsprincipes en verantwoordelijkheidsstructuren van het openbaar bestuur? Wat betekent digitalisering in essentie voor de normatieve oriëntaties die ten grondslag liggen aan de taakuitoefening door de overheid? Of, anders geformuleerd: wat mogen burgers nu precies verwachten van de, veelal zeer aanbodgestuurde, inzet van ICT door de overheid en wat betekent dat voor taakopvatting

en bestuurlijke inrichting? In hoeverre zet de toenemende digitale mondigheid en assertiviteit van burgers de positie en rol van de publieke sector onder druk? Hoe en op welke wijze moet de balans worden gevonden tussen belangrijke waarden als efficiëntie, veiligheid en privacy?

Wie zich het antwoord op deze vragen en meer algemeen het 'lot' van digitalisering speciaal moet aantrekken (en hoe) is echter een verre van eenduidige kwestie. Sterker nog: digitalisering anno 2011 lijkt vaak van iedereen en niemand. Dat geldt zowel voor de digitalisering binnen de overheid als voor de digitalisering van de bredere samenleving. Deze constatering verdraagt zich echter slecht met de bijzondere positie die de overheid in termen van macht en verantwoordelijkheid inneemt. Ook in een digitale wereld is het borgen van publieke belangen immers aan de orde, wat eisen stelt aan het nemen en organiseren van verantwoordelijkheid. De overheid ontkomt niet aan een spagaat: de inzet van ICT door de overheid moet het leven van burgers in diverse opzichten aangenamer en veiliger maken, maar zij moet ook waken over fundamentele rechten zoals privacy en autonomie van burgers.

1.2 EEN iOVERHEID

De zoektocht naar deze spagaat vormt het vertrekpunt van dit rapport. Digitalisering heeft zowel de samenleving als de overheid op ingrijpende wijze veranderd en confronteert ons met een diversiteit aan fundamentele kwesties. Een groot aantal daarvan raakt in essentie aan de rol en verantwoordelijkheid van de overheid. Digitalisering bij de overheid vindt niet plaats in een vacuüm, maar is nauw verweven met veranderingen die op brede schaal plaatsvinden in de informatiesamenleving. De mogelijkheden die ICT biedt om informatie samen te brengen, te delen en in tal van domeinen in te zetten, maakt dat verwachtingen en verantwoordelijkheden van zowel overheid als burgers veranderen. Het is daarom zaak te onderzoeken hoe de relatie overheid-burger(s) onder invloed van ICT feitelijk is veranderd, en wat daarvan de praktische en normatieve implicaties zijn. Die implicaties zullen deels in de categorie 'accepteren van en aanpassen aan een veranderde situatie' vallen, maar deels ook nopen tot bijstellingen op een meer fundamenteel niveau. De huidige digitalisering van de samenleving en overheid en het onevenwichtige politiek-bestuurlijke debat daarover, vragen daarmee om een analyse van en perspectief op alsmaar voortschrijdende ontwikkelingen. Op zichzelf is de oproep tot een (institutionele) aanpassing al eerder gedaan, ook vanuit door de overheid zelf geïnitieerde programma's, zoals het Infodrome-project: "Dus is het zaak om nu na te denken over de inrichting van de informatiesamenleving" (Infodrome 2001: 165; zie ook de diversiteit aan adviezen besproken in Rob 2003). Maar tot op heden heeft de overheid de uitdaging tot het ontwikkelen van een politieke agenda voor de informatiesamenleving niet ter hand genomen.

Dit rapport concludeert dat niet langer met de noodzakelijke transformatie kan worden gewacht. Aan de hand van een uitgebreide empirische analyse van de digitaliseringsinitiatieven van de (in hoofdzaak Nederlandse) overheid duidt dit rapport de realiteit van de 'elektronische overheid'. Geconstateerd wordt dat de overheid onder invloed van digitalisering ingrijpend van karakter is veranderd. De overheid functioneert niet alleen tegen de achtergrond van een informatiesamenleving, maar is zelf een informatieoverheid, een *iOverheid*, geworden. De facto en bijna ongemerkt heeft zich een praktijk ontwikkeld, waarin samenhangende informatiestromen het karakter van de overheid domineren. En daarmee bepalen deze informatiestromen ook het functioneren, de afhankelijkheid en de kwetsbaarheid van zowel de overheid als haar burgers. In de dagelijkse werkelijkheid van politiek en bestuur wordt echter allesbehalve vanuit het samenhangende idee van deze iOverheid gedacht en gewerkt: het overgrote deel van de overheidsinitiatieven voor digitalisering – applicaties als het biometrisch paspoort of het EPD – en de informatiestromen die daaruit volgen, worden geïsoleerd bepleit, beoordeeld en ingevoerd. Individuele initiatieven worden niet of nauwelijks beoordeeld op hun (potentiële) invloed op de overheid en de samenleving als geheel. Ook worden ze niet of nauwelijks bezien vanuit het perspectief van de snel groeiende en vertakkende informatiestromen. De iOverheid staat zogezegd niet op het netvlies van politiek en beleid. Juist daarom ook ontbreken de verantwoordelijkheidsstructuren en het beleidsinstrumentarium om de iOverheid op een zorgvuldige en innovatieve manier verder te ontwikkelen. Wil de overheid echter in de toekomst het pad van digitalisering met vertrouwen kunnen vervolgen, dan zal het perspectief verlegd moeten worden en wel – in de termen van dit rapport – van de eOverheid naar de iOverheid. Vanuit deze opdracht ontwikkelt deel III een inhoudelijke en institutionele agenda, waarbij de nadruk ligt op de vernetwerkte informatiehuishouding van de overheid.

Hoewel dit rapport de ontwikkeling van de iOverheid dus als centraal thema heeft en daarmee in hoofdzaak gaat over de rol en de verantwoordelijkheid van de overheid bij de inzet van ICT voor het eigen beleid, kan dit betoog niet los worden gezien van de bredere context van de ontwikkelingen in de informatiesamenleving. De informatiesamenleving vormt het decor voor de analyse van de inzet van ICT door de overheid. De digitale dynamiek in de samenleving bepaalt immers mede de kansen, beperkingen en opgaven voor de iOverheid. De volgende paragraaf staat dan ook allereerst stil bij een aantal vitale ontwikkelingen die van betekenis zijn voor de belangen en rollen van overheid en burgers.

1.3 DE iSAMENLEVING

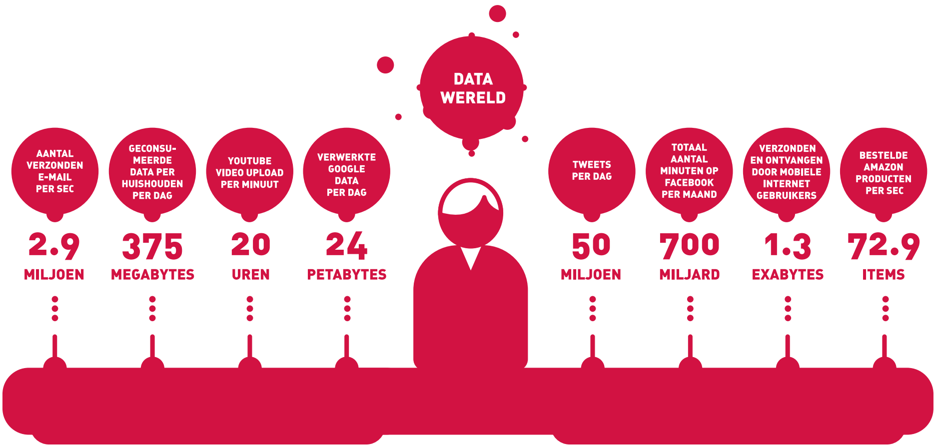
Digitalisering verandert de samenleving ingrijpend, zonder dat daarvoor één doorslaggevende factor is aan te wijzen (Dutton 1999). De verscheidenheid van factoren komt terug in de typeringen die de 'nieuwe' samenleving moeten duiden:

naast informatiesamenleving wordt er ook gesproken van een netwerksamenleving en kennissamenleving. Al deze benamingen verwijzen, met verschillende accenten, naar tendensen die relateren aan digitalisering of informatisering, onderlinge relaties en verbondenheid in netwerken. De consequenties van de inzet van ICT voor de relatie van overheid en burgers hangen samen met ontwikkelingen in de bredere context van de informatiesamenleving (iSamenleving). Zo is het web gestaag, vanaf eind jaren negentig van de vorige eeuw, voor vele gebruikers het middel bij uitstek geworden om informatie te zoeken en te verspreiden, maar ook om zelf nieuwe inhoud te creëren, steeds vaker in samenwerking met anderen. In 2006 koos het tijdschrift *Time* dan ook niet voor een groot politicus, wetenschapper of artiest als 'persoon van het jaar', maar voor 'YOU', de verzameling van interactieve individuen die, gebruikmakend van het internet, de wereld naar hun hand zetten (zie ook Frissen 2008).

In korte tijd zijn er invloedrijke nieuwe spelers op het toneel verschenen, zoals Google, Facebook en Flickr, die specifiek inspelen op de behoeften van gebruikers om informatie te zoeken en te delen en om sociale interacties op het web aan te gaan. De spelers van de nieuwe 'informatie-economie' (Van der Laan & De Haan 2005: 13-14) lanceerden nieuwe, ongekende digitale diensten en wisten de informatie die daarmee wordt verzameld om te zetten in jaarlijkse winst of in ieder geval een aantrekkelijke beurswaarde. Achter de schermen werken duizenden systeembouwers aan de uitbouw van de informatiesamenleving en evenzoveel adviseurs ondersteunen bedrijven en overheden bij de ontwikkeling en implementatie van hun digitaliseringsambities. Vrijwel al deze ambities draaien, zoals figuur 1.2 al schetst, om het vermogen met grote hoeveelheden informatie te innoveren, hetzij voor het publieke belang, hetzij voor het private belang. Castells (1996) kwalificeerde de basis van de netwerkmaatschappij meer dan een decennium geleden al als een informationele kapitalistische economie, in tegenstelling tot een voornamelijk industriële kapitalistische economie die daaraan voorafging.

Deze ontwikkelingen in de samenleving raken natuurlijk ook de overheid. De toenemende mogelijkheden om via ICT gemakkelijk en snel informatie te delen, houden voor de bedrijfsvoering van de overheid de belofte in van een verhoogde effectiviteit en efficiëntie. Tegen het einde van de twintigste eeuw is het wetenschappelijke en beleidsdiscours vervuld van de mogelijkheid om met behulp van ICT de overheid efficiënter, effectiever en klantvriendelijker te maken (Boersma et al. 2009; Dunleavy et al. 2006; Van de Donk & Van Dael 2005). ICT wordt in de ogen van de overheid het middel bij uitstek om te innoveren en te vernieuwen. Deze ambitie kreeg al snel de benaming *electronic government* (eGovernment of eOverheid) mee. De eGovernment-gedachte is wereldwijd opgepakt door overheden, al leggen landen hierbij wel verschillende accenten en komen ze tot verschillende resultaten (Lenk & Traunmüller 2007; Dunleavy et al. 2006; Mayer-Schönberger & Lazer 2007; Boersma et al. 2009 en de verschillende landenstudies in Prins 2007).

Figuur 1.2 Informatiestromen in de iSamenleving



Gebaseerd op gegevens van Cisco, Comscore, Mapreduce, Radicatie Group, Twitter, Youtube.
Bron: *Good Magazine*/Oliver Munday/IBM

In de iSamenleving wordt digitalisering ingezet om ambities, zowel publiek als privaat, voor het vernieuwen en verbeteren van processen en relaties te realiseren. Maar de inzet van informatie en technologie brengt naast bedoelde, ook onbedoelde effecten met zich mee. Informatisering heeft vaak verstrekkende gevolgen die niet allemaal voorzien en van tevoren doordacht zijn. In deze paragraaf komen enkele belangrijke kenmerken van de iSamenleving aan de orde, namelijk: de innoverende kracht van ICT, de sociale kracht van ICT die veranderingen in relaties en verhoudingen met zich meebrengt, en de kansen en risico's ten aanzien van veiligheid en kwetsbaarheden van digitale sporen. Deze ontwikkelingen vormen een belangrijk deel van het decor waartegen de iOverheid zich heeft ontwikkeld en zich verder zal ontwikkelen.

Vernieuwen en verbeteren: de innoverende kracht van ICT

De opmars van ICT in ons dagelijks leven komt niet uit de lucht vallen. Van oudsher is de ontwikkeling van de mens onlosmakelijk verbonden met de ontwikkeling van de technologie. Het vermogen om functies uit te besteden aan technologie (of het nu gaat over 'simpele' techniek en werktuigen of over complexe artificiële intelligentie) heeft de menselijke ontwikkeling altijd al bepaald. De wens de wereld om ons heen te kunnen beheersen en controleren, gecombineerd met een groot vertrouwen in de mogelijkheden van technologie om dat te doen, heeft ervoor gezorgd dat ICT vaak uit de bus komt als de ultieme oplosser voor tal van maatschappelijke problemen. Bovendien verwachten mensen ook dat technologische hulpmiddelen daadwerkelijk worden ingezet (De Haan 2004). Zo wordt de roep om veiligheid beantwoord met bewakingscamera's, biometrische toegangscontroles en hightechdefensiematerieel. De vraag naar meer efficiëntie wordt

beantwoord door dienstverlening naar het web te migreren, zodat het 'loket' vierentwintig uur per dag beschikbaar is, en databases worden zodanig opgetuigd dat gegevens gemakkelijk verzameld, gecombineerd en vervolgens uitgewisseld kunnen worden. In eerste instantie heeft vooral het bedrijfsleven de nieuwe mogelijkheden van ICT opgepakt (De Haan et al. 2005).

Mede onder invloed van de ontwikkelingen in de private dienstverlening en de belofte van effectiviteit en efficiëntie zette ook de overheid in de jaren negentig van de vorige eeuw de eerste schreden op het digitaliseringspad. De overgang naar een elektronische overheid werd gepresenteerd als wenselijk, maar ook als onvermijdelijk: "Een vitale maatschappij met een gezonde economie vraagt om een sterke overheid, die haar rol vervult met de meest geavanceerde 'gereedschappen' die er zijn" (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) 1998: 3). Het streven om de overheid om te vormen naar een elektronische overheid past bij twee trends die eind jaren tachtig steeds dominanter werden in het denken over overheid en publieke sector (Bekkers & Zouridis 1999; Fountain 2001). Ten eerste wordt het openbaar bestuur, onder de financiële druk van een sterk gegroeide verzorgingsstaat, steeds vaker beschouwd als een bedrijf (Noordegraaf et al. 1995). In deze *New Public Management*-benadering spelen publieke managers, bedrijfsmatige instrumenten, efficiëntie en dienstverlening een grote rol in het openbaar bestuur. De tweede trend hangt samen met een verschuiving van een focus op de sturende, faciliterende en ordenende rol van de overheid naar een focus op de rol van de overheid als actieve speler (Bekkers & Homburg 2009). In de beginfase van de eOverheidsontwikkeling wordt voornamelijk ingezet op het vergroten van de toegankelijkheid van de overheid, het verhogen van de kwaliteit van dienstverlening en efficiëntere interne processen (Ministerie van BZK 1998; Ministerie van Economische Zaken (EZ) 1999). Maar al spoedig gaan koplopers zoals Zweden, Denemarken, Noorwegen, de Verenigde Staten, maar ook Nederland een stap verder door te investeren in onder meer een geïntegreerde backoffice die niet alleen efficiëntere, maar ook proactieve dienstverlening mogelijk moet maken. De titel van de e-Government Survey 2008 van de Verenigde Naties (2009) *From e-government to connected governance* is tekenend voor deze ontwikkeling. Het rapport noemt als een belangrijk kenmerk van deze netwerkoverheden het vermogen om door middel van ICT informatie gelijktijdig uit verschillende departementen en domeinen op te roepen om zo op een adequate manier te kunnen reageren op actuele vragen en problemen (Verenigde Naties 2009: 8).

Betere dienstverlening betekent dus aanvankelijk, passend in het New Public Management-denken, voornamelijk efficiëntere dienstverlening. De overheid presenteert zich als de producent van diensten voor de burger als consument (Fountain 2001) en meet haar vooruitgang aan de hand van kwantitatieve doelstellingen: zoveel procent van alle dienstverlening moet langs elektronische weg worden verstrekt (Bekkers 2001). In de begindagen van eOverheid wordt dan ook

vooral gesproken over dienstverlening *van* de overheid *aan* de burger. Maar onder invloed van de opkomst van het 'sociale' web en zijn groeiende betekenis binnen de iSamenleving, verschuift ook binnen de overheid de aandacht naar mogelijkheden van participatie van en cocreatie met burgers. De burger kan naast consumeren ook produceren.

Online deelname: de sociale kracht van ICT

Internet is in Nederland geen randverschijnsel meer: het Centraal Bureau voor de Statistiek (CBS) heeft uitgerekend dat inmiddels bijna twaalf miljoen mensen in Nederland regelmatig gebruikmaken van internet (CBS 2009a). Zowel in termen van computerbezit als internettoegang is Nederland koploper in de Europese Unie. In 2009 heeft 93 procent van de Nederlandse bevolking thuis toegang tot een computer en heeft bijna acht op de tien Nederlanders thuis een internetaansluiting (CBS 2009a). Het probleem van de digitale kloof tussen gebruikers en niet-gebruikers is hiermee verschoven van toegang naar vaardigheden. Vaardigheden, te onderscheiden in technische en formele maar ook strategische en informatie vaardigheden (Van Deursen & Van Dijk 2010), zijn bijzonder relevant wanneer de gebruiker niet langer uitsluitend consument is, maar ook producent.

De verschuiving van consument naar producent is kenmerkend voor wat met 'web 2.0' wordt aangeduid: individuen hebben de mogelijkheid om via tal van internetapplicaties en mobiele media samen te werken aan zogenaamde cocreaties. Mensen onderhouden zonder centrale organisatie en aansturing online sociale relaties, delen kennis en ideeën of werken samen aan projecten, zoals aan de online encyclopedie Wikipedia. Omdat voor de populaire web 2.0-applicaties zoals LinkedIn en interactieve games geen aparte software geïnstalleerd hoeft te worden, maar het internet als platform functioneert, zijn de nieuwe diensten en applicaties zeer laagdrempelig en voor een groot publiek bereikbaar. Met de komst van de interactieve mogelijkheden deed het 'sociale web' zijn intrede. Dat online sociale netwerken aan belang winnen, valt cijfermatig op te maken uit het feit dat meer dan één op de vier personen die op het net surft een Facebook-account heeft en dat account bovendien de afgelopen maand nog heeft bezocht (Facebook 2010). Facebook kent momenteel wereldwijd meer dan 500 miljoen deelnemers. De Nederlandse tegenhanger Hyves mag er ook zijn: medio juni 2010 telde deze site 10.2 miljoen leden (Hyves 2010).

Het groeiende gebruik van *social network sites* als Hyves en Facebook maakt overstappen naar of aansluiten bij die toepassing aantrekkelijker. De populariteit van een dergelijke applicatie in de samenleving dicteert als het ware een technologisch pad voor nieuwe, maar ook bestaande gebruikers (Mulder 2006: 115). Het aanmaken van een Hyves- of Facebookprofiel is immers alleen interessant wanneer er ook anderen zijn waarmee je in contact kan treden. De ontwikkeling van een nieuwe technologie als zodanig is dan ook nooit de enige aanzet tot verandering (Van der Laan & De Haan 2005: 13). Ontwerpers, bedrijven en producenten mogen

nog zulke mooie applicaties ontwerpen, het zijn uiteindelijk de gebruikers die er het nut en gebruikersgemak van moeten inzien en het product maken of breken.

De populariteit van het internet is overduidelijk, maar toch is enige nuancering van met name het 'sociale web' op zijn plaats. Niet iedereen die op het web surft is immers even actief. Eenderde van de internetgebruikers beperkt zijn activiteit voornamelijk tot het lezen van blogs, het bekijken van filmpjes op YouTube of het bezoeken van websites zoals Wikipedia (Frissen et al. 2008). Om en nabij de tien procent van de internetgebruikers levert feedback door bijvoorbeeld commentaar te geven op een online krantenartikel of een boekrecensie te schrijven bij bol.com. Nog eens tien procent deelt informatie, bijvoorbeeld foto's via Flickr of muziek via MySpace. Als het gaat om het zelf creëren van inhoud (bijvoorbeeld door te bloggen of Wikipedia-artikelen te schrijven), is slechts drie procent van de internetters actief (Frissen et al. 2008). Bovendien is er ook een groep mensen die er bewust voor kiest een niet-gebruiker te zijn, omdat men geen zin of tijd heeft, geen vertrouwen heeft in de applicatie of er simpelweg het nut niet van inziet (Van Dijk 2007; Van den Berg 2008; Wyatt 2003).

Een tweede nuancering betreft de idee van het web als een grote vrijplaats waar iedereen kan doen en laten wat hij of zij wil (Zittrain 2008; Anderson & Wolff 2010). Er is een overgang merkbaar van het open web naar verschillende semigesloten platforms zoals Facebook of LinkedIn. In plaats van het hele web te doorzoeken, klikken gebruikers meteen door naar de voor hen bekende en vertrouwde website. De opkomst van smartphones, iPhones en iPads werkt deze manier van zoeken en vinden verder in de hand. Via deze *mobile devices* is het immers kinderlijk eenvoudig om via het aantikken van aparte icoontjes direct de gewenste informatie te raadplegen. Dat wat het gebruik van deze platforms zo aantrekkelijk maakt voor gebruikers – de eenvoudige manier waarop informatie gedeeld kan worden en interacties aangegaan kunnen worden – is tegelijkertijd de sleutel tot het succes van de bedrijven die deze platforms opzetten. Afgesloten systemen zijn nu eenmaal beter te controleren dan vrijplaatsen, en daarmee een betrouwbaarder investering (Zittrain 2008). Informatie van en over de gebruikers is de grondstof van hun business. Het in grote hoeveelheden verzamelen, verrijken, benutten en ook verder doorverkopen van informatie maakt gepersonaliseerde reclame en diensten mogelijk (Lips et al. 2005).

Digitale verhoudingen: ICT doet posities verschuiven

De komst van web 2.0 en de daarmee samenhangende invloed van de *crowd* raakt ook het doen en laten van de overheid (Frissen et al. 2008). Onder de noemer e-participatie proberen verschillende overheidsonderdelen de potentie van burgerbetrokkenheid te benutten. Het web maakt communiceren en cocreëren mogelijk en kan dus in potentie veel verdergaan dan uitsluitend het informeren van burgers. Het biedt de mogelijkheden voor een wederkerige relatie van mobiliseren, stimule-

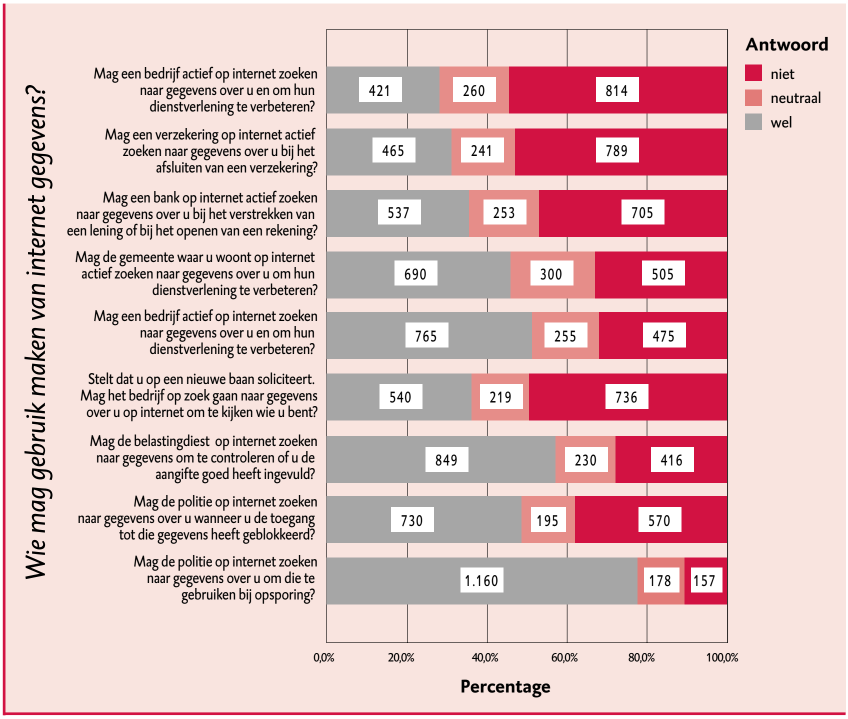
ren, creativiteit en betrokkenheid (Bekkers & Thaens 2002; Bekkers & Meijer 2010). Voor de overheid kan het web een sleutel zijn tot het vinden van een nieuwe rol die past bij de "fragmentatie van de samenleving als gevolg van een voortgaand proces van differentiatie, specialisatie en professionalisering" (Bekkers & Meijer 2010: 9). Het zoeken naar nieuwe manieren om met burgers in contact te komen, is een van de antwoorden op het 'kloof-denken' dat het discours over legitimiteit van de overheid steeds meer is gaan beheersen (zie o.a. Andeweg & Van Gunsteren 1994; Tiemeijer 2006; Van Gunsteren 2006; Chavannes 2009; Verhoeven 2009; Rob 2010a). De veronderstelde kloof tussen bestuur en burger – opgehangen aan indicaties van politiek wantrouwen, lage opkomstpercentages bij verkiezingen en lage waarderingscijfers van politici – stelt de legitimiteit van de overheid om maatschappelijke uitdagingen aan te pakken ter discussie. Om dit tij te keren wordt ICT gezien als het middel bij uitstek om via e-participatie de legitimiteit van politiek en beleid te versterken.

Hoewel Nederland momenteel bij de top vijf van de wereld hoort als het gaat om eOverheidsontwikkelingen en het ook niet slecht doet op het vlak van e-participatie met een met Frankrijk gedeelde vijftiende plaats (Verenigde Naties 2010), liggen er nog vele onbenutte kansen. Er valt winst te behalen in de mate waarin de overheid informatie deelt (bijvoorbeeld door beleidsteksten te publiceren), burgers consulteert (bijvoorbeeld aangaande wetgeving), en burgers laat meebeslissen (Verenigde Naties 2010). Ook mogelijkheden om vorm te geven aan een nieuwe verhouding tussen overheid en burgers, waarbij de overheid en de politiek niet meer als vanzelfsprekend op basis van een verkregen mandaat van een grote groep burgers beslissingen nemen, maar waarbij kritische (individuele) burgers zelf participeren in beleidsvormings- en besluitvormingsprocessen, blijven vooralsnog onbenut.

De bovengenoemde kansen die ICT voor onder meer inspraak, participatie en cocreatie biedt, brengen voor de overheid ook problemen met zich mee. Veranderingen in de rol en positie van verschillende actoren stellen de overheid voor de vraag hoe ze hierop dient te reageren. Internet biedt burgers de mogelijkheid om zelfstandig de overheid te controleren en als *countervailing power* in de publieke arena op te treden (Meijer 2004). Zo maakt een voorhoede van digitale burgers, in Nederland bestaande uit organisaties als Het Nieuwe Stemmen, Bits of Freedom, PrivacyFirst, NLnet en Internet Society, zich sterk voor een transparante overheid. Deze nieuwe generatie burgers wil bijvoorbeeld met één druk op de knop kunnen volgen hoe hun volksvertegenwoordigers stemmen. En als de overheid niet voor deze transparantie zorgt, dan doen de georganiseerde burgers dat wel zelf, zoals het burgerinitiatief Watstemtmijnraad.nl – een website waarop te zien is hoe er in een gemeente wordt gestemd – illustreert. Naast organisaties die wedijveren voor een digitaal volwassen overheid, wijzen instanties als Burgerlink op de negatieve gevolgen van het digitale imperatief. Zij maken zich sterk voor het openhouden van andere (dus ook de traditionele) communicatiekanalen naast het snel opkomende digitale kanaal, om zo de keuzevrijheid van de burger te vrijwaren.

De oproep vanuit een groeiend aantal organisaties tot een kritische reflectie op de reikwijdte en implicaties van de digitalisering in de samenleving, en in het bijzonder bij de overheid, is niet specifiek voor Nederland. Sterker nog, wie over de grenzen kijkt, bijvoorbeeld naar Duitsland en de Verenigde Staten, ziet een vele malen levendiger en kritischer maatschappelijk debat. Over het algemeen kan het debat in Nederland op weinig maatschappelijke bijval rekenen. Dat valt gedeeltelijk te verklaren uit het vertrouwen dat Nederlandse burgers stellen in het ICT-gebruik van de overheid. Uit een enquête die de WRR in samenwerking met het Platform voor InformatieSamenleving (ECP-EPN) en Centerdata heeft gehouden, blijkt dat burgers in hoge mate vertrouwen hebben in de wijze waarop de Nederlandse overheid gebruikmaakt van ICT en omgaat met informatie. Zo krijgt de overheid (opsporing, Belastingdienst) van respondenten aanzienlijk meer ruimte om gegevens te gebruiken dan het bedrijfsleven (Attema & De Nood 2010: 2). Meer dan 60 procent is voor digitale registratie in het algemeen, en digitale registratie in de gezondheidszorg kan op instemming van bijna 80 procent van de respondenten rekenen. Slechts 10 procent van de respondenten geeft expliciet aan tegen digitale registratie te zijn (Attema & De Nood 2010: 3).

Figuur 1.3 Meningen over informatiegebruik door publiek en private actoren



Bron: Attema en De Nood 2010: 3

In Duitsland daarentegen stappen burgers naar de rechter vanwege de Europese bewaarplicht van verkeersgegevens en sturen ze massaal boze e-mails naar de Europese Ombudsman wanneer het bericht opduikt dat er een surveillancesysteem (genaamd Enfopol) in de maak zou zijn. Ook in Amerika zetten private en publieke organisaties (zoals EPIC en de Electronic Frontier Foundation), maar ook individuele burgers overheden onder druk om meer openheid van zaken te geven, zoals bijvoorbeeld recentelijk over de ACTA-onderhandelingen (een omstreden plan onder meer om internetpiraterij te bestrijden). Dat deze zorgen van burgers niet aan dovemansoren gericht zijn, illustreert het Open Government[1] initiatief dat president Obama vrijwel direct na zijn aantreden voor de gehele Amerikaanse federale overheid afkondigde. Ook in het Verenigd Koninkrijk komen projecten voor Open Data van de grond.[2] Op Europees niveau wordt transparantie gezien als een noodzaak voor participatieve democratie in een informatiesamenleving en als voorwaarde voor legitiem overheidsoptreden (Europese Commissie 2001). Vanuit die gedachte worden documenten van de Europese Instellingen online beschikbaar gesteld en wordt inspraak in wetgevingsprocessen gestimuleerd. Lor & Britz (2007) stellen dat vrije toegang tot informatie onontbeerlijk is voor burgers om te kunnen participeren in een wereld waarin informatie zo een cruciale rol speelt. Deze vrijheid van informatie wordt ook wel benoemd als 'Het recht op informatie' en kent zijn uitwerking in talloze nationale en internationale wetgeving (vgl. Singh 2007; Horsley 2007). Ook in Nederland zet de overheid – zij het schoorvoetend – in op meer burgerbetrokkenheid bij beleidsvorming en daarmee ook transparantie, getuige onder meer het initiatief internetconsultatie ten behoeve van wetgeving.[3]

Digitale sporen: een paradox van veiligheid en kwetsbaarheid

Met de groei van het digitaal uitwisselen en delen van informatie nemen ook de digitale sporen van burgers toe. Wanneer informatiestromen een steeds prominentere plaats in het handelen van bedrijven en overheden innemen, heeft dit consequenties voor het gedrag van personen en de digitale sporen die dat achterlaat. Surveillance, *data mining* en *profiling* zijn moderne technologische toepassingen die de digitale sporen gebruiken als grondstof voor het volgen van personen en ontwikkelingen en het opsporen van bijvoorbeeld (potentieel) onveilige situaties of personen (House of Lords 2009). De ultieme informatiesamenleving is een transparante maatschappij (Tsoukas 1997) en biedt volop kansen om 'informatiegestuurd beleid' te ontwikkelen, maar brengt ook nieuwe kwetsbaarheden met zich mee voor burgers (onterecht als verdachte behandeld) en overheden (onterecht vertrouwen op statistische 'zekerheden').

De nadruk op de kansen die technologie en informatie bieden voor het vergroten van de effectiviteit en efficiëntie van (overheids)optreden blijft niet beperkt tot het streven naar een dienstverlenende overheid. Ook voor maatschappelijke en sociale veiligheid wordt de inzet van ICT in toenemende mate sterk gepropageerd en gebruikt. De aanslagen in New York, Madrid en Londen hebben zowel de angst

versterkt als het politieke ambitieniveau om nationale veiligheid en bestrijding van terrorisme hoog op de nationale en internationale politieke agenda's te zetten en in concrete acties om te zetten (Lyon 2003; Edwards & Meyer 2008). Belangrijke wapens in de strijd tegen terrorisme zijn mogelijk dankzij nieuwe technologie, bijvoorbeeld op het gebied van biometrie, data-analyse en informatieopslag en -uitwisseling. Voor de uitvoering zijn nieuwe organisaties opgericht of bestaande inlichtingendiensten op informatieniveau met elkaar versmolten. Waar de Verenigde Staten hebben gekozen voor een institutionele oplossing door het oprichten van het Department of Homeland Security, opteerde Europa voor het intensief uitwisselen van informatie tussen de verschillende inlichtingendiensten (Müller-Wille 2008). Naast deze structurelere antwoorden op de dreiging gaven incidenten aanleiding tot het nemen van allerlei ad-hocveiligheidsmaatregelen. Zo leidden de door MI5 ontdekte plannen voor aanslagen met behulp van vloeistoffen in 2006 en de 'onderbroekbom' die een Nigeriaanse man op 25 december 2009 probeerde te ontsteken tijdens een vlucht van Amsterdam naar Detroit, tot het verbod op onverpakte vloeistoffen in de handbagage en de invoering van de *total body scan* op luchthaven Schiphol (Van Eeten 2011). Paradoxaal vormen technologische innovaties zowel voor de terrorist als voor de politicus een instrument om, weliswaar met diametraal tegenovergestelde doelstellingen, daadkracht te tonen.

Informatie komt steeds naar voren als een belangrijk wapen om internationale veiligheid te bewerkstelligen. Data mining, profiling en de automatisering van gegevensbestanden heeft in de laatste tien jaar dan ook een grote vlucht genomen (Lyon 2003; Adviescommissie Informatiestromen Veiligheid 2007; Müller-Wille 2008; Balzacq 2008). Niet alleen voor mondiale veiligheid, maar ook voor veiligheid dicht bij huis, of zelfs achter de voordeur, wordt slim gebruik van informatie en technologie steeds meer gezien als een belangrijke voorwaarde voor succesvol beleid. De toepassingen zijn legio en divers – cameratoezicht, gezichtsherkenningssoftware in het openbaar vervoer, metaaldetectoren bij uitgaansgelegenheden, biometrische vingerafdrukken in het paspoort en een nationale database, Elektronisch Kinddossier, Verwijsindex Risicojongeren – en kunnen veelal rekenen op maatschappelijke instemming. Zo blijkt uit het rapport *In het Zicht van de Toekomst* van het Sociaal en Cultureel Planbureau (2004) dat ruim 85 procent van de Nederlanders de inzet van camera's prima vindt en zelfs bijna 100 procent de ruimere toepassing van DNA-onderzoek om de identiteit van daders vast te stellen, een goede zaak vindt. Recenter onderzoek van het Rathenau Instituut, ecp.nl en de Consumentenbond (Rathenau Instituut et al. 2007) laat zien dat de Nederlandse bevolking welwillend staat tegenover de inzet van digitale persoonsinformatie voor opsporingsdiensten. Ruim de helft (56%) bleek voor, 26 procent tegen en 18 procent onbeslist als het gaat om de mogelijkheid pasfoto's gedigitaliseerd voor opsporing op te slaan. Bij eenzelfde vraag over vingerafdrukken, in een recenter onderzoek, was er zelfs nog meer instemming: 66 procent voor, 20 procent tegen en 14 procent wist het niet (Van het Hof et al. 2010: 93).

Maar ook breder dan gericht op terrorismebestrijding en criminaliteitsbeheersing is veiligheid een populair publiek en politiek thema in de moderne westerse maatschappij, denk bijvoorbeeld aan terreinen als (gezondheids)zorg of verkeer en milieu. Veiligheid, of liever onveiligheid, scoort hoog in bevolkingsonderzoeken (CBS 2009b) en de zorg van de overheid voor (fysieke, internationale, sociale) veiligheid heeft zich gestaag uitgebreid, hetgeen zichtbaar is in toenemende budgetten, toenemende regeldruk en toenemende uitvoerings- en coördinatieproblemen (WRR 2008b). De overheid ziet het steeds meer als haar taak om veiligheid actief te bevorderen door risico's te voorkomen en proactief op te treden in domeinen als jeugdzorg (Prins 2009; Schinkel 2009; Keymolen & Prins 2011), gezondheidszorg (Keizer 2011; Pluut 2010) en verkeer (Potters & De Vreeze 2010). Frissen (2009) constateert op terreinen als openbare orde, veiligheid, jeugdzorg, opvoeding en integratie dat maakbaarheid als ideologie tot uiting komt in een bijzondere combinatie van preventie en repressie. Het beleid krijgt in termen van ambitie, reikwijdte en pretenties steeds meer een totaal en omvattend karakter (zie ook Van Gunsteren 2004).[4]

Technologie wordt ingezet om risico's te beheersen en controleren, en op de langere termijn om schade te voorkomen. Beck (1992) verwijst met de term risicomaatschappij naar de tendens dat hoe meer het technologisch mogelijk is om risico's te voorkomen, hoe minder mensen nog accepteren dat het ook wel eens fout kan gaan. De behoefte aan controle en aan (sociale) veiligheid is mede gegroeid omdat hiërarchische structuren plaatsmaken voor netwerkstructuren. De roep om aandacht voor veiligheid en de behoefte aan controle hangen samen met processen van decentralisering en privatisering, waarbij verantwoordelijkheden zijn verspreid over tal van organisaties en instituties. In een poging de risico's te beheersen en controleren is de moderne samenleving in de ban geraakt van veiligheidsdenken. Boutellier (2003: 67) spreekt van een veiligheidsutopie, oftewel "(...) het (onhaalbare) streven naar een optimale samenhang tussen vitaliteit en veiligheid. De risicosamenleving heeft zijn eigen utopie gebaard, namelijk de vereniging van twee tegengestelde behoeften: vrijheid en veiligheid." Dat verlangen wordt keer op keer bevestigd door incidenten en de daaropvolgende reactie van media en politici (Van Eeten 2011).

Technologie, ICT in het bijzonder, maakt echter niet alleen handhaving en controle mogelijk, het faciliteert ook nieuwe vormen van criminaliteit en maakt de samenleving daarmee op geheel nieuwe wijze kwetsbaar. *Cybercrime, phishing*, creditcardfraude, identiteitsdiefstal: het zijn allemaal vormen van criminaliteit die met de komst van digitalisering hun intrede hebben gedaan. Het Britse Crime Prevention Panel spreekt over "digitalisering van de criminaliteit" (SCP 2004: 475). Govcert (2010), de overheidsorganisatie die onder meer waakt over de veiligheid op internet, meldt in het jaarverslag 2009 dat de online criminaliteit sterk groeit. Een belangrijke oorzaak ligt bij de toenemende populariteit van het internet voor

het afhandelen van allerhande dagelijkse beslommeringen (bestellen, betalen), waardoor digitale criminaliteit een steeds lucratievere bezigheid wordt voor criminelen. De *Verkenning Cybercrime in Nederland 2009* concludeert aan de hand van vijf vormen van cybercrime (hacken, e-fraude, cyberafpersen, kinderpornografie en haatzaaien) dat cybercrime 'van het volk' is. Terwijl de media, beleidsdocumenten en literatuur een beeld schetsen van hightech- en georganiseerde criminelen, blijkt uit onderzoek van 665 politiedossiers juist dat er veel 'kleine' delicten worden gepleegd door min of meer alledaagse verdachten die individueel opereren (Leukfeldt et al. 2010). De toenemende kwetsbaarheid raakt overigens niet alleen burgers. Ook de overheid zelf wordt, zo waarschuwt de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2010a; 2010b) steeds vaker slachtoffer van digitale criminaliteit en spionage. Binnen de overheid bestaat echter onvoldoende aandacht voor en daarmee ook besef van deze eigen kwetsbaarheid, zo merken diverse gesprekspartners van de WRR op.[5]

Burgers dragen ook zelf bij aan het ontstaan van nieuwe kwetsbaarheden. Profielen op *social network sites* bevatten vaak persoonlijke details en gebruikers zijn zich niet altijd bewust wie welke gegevens kan inzien (Boyd 2008). Al dan niet legale softwareprogramma's als spyware 'houden in de gaten' naar welke websites er wordt gesurft en op welke links er wordt geklikt. Zowel private als publieke organisaties huren bedrijven in om het bezoekgedrag van gebruikers van hun websites te analyseren. Via het internet verzamelde informatie wordt bovendien vaak in grote hoeveelheden verkocht met onder meer als doel gepersonaliseerde reclame en diensten mogelijk te maken. Digitale sporen laten gebruikers echter niet alleen via het internet achter. Ook via mobiele telefoons, navigatiesystemen in auto's, digitale passen en poortjes en zelfs zeer kleine chips aangebracht in allerlei consumentenartikelen die signalen uitzenden (*radio-frequency identification* (RFID)), kunnen het gedrag en de handelingen van personen in kaart worden gebracht (Van Est et al. 2007; Van 't Hof et al. 2010). Zo is de OV-chipkaart ontworpen om naast een betaalsysteem, ook een systeem op te leveren dat de reizigersstroom inzichtelijker en beter beheersbaar maakt. Het systeem registreert en analyseert de reisgegevens en geeft die informatie door aan andere betrokkenen binnen het OV-chipkaartsysteem: de vervoerders, tussenpartijen, overheden en de reiziger zelf (Van 't Hof et al. 2010; Griffioen 2011).

Dat met deze ontwikkeling ook vragen omtrent privacy, veiligheid en transparantie rijzen wordt steeds duidelijker. Google en Facebook zijn regelmatig in het nieuws als het om privacyinbreuken gaat (Olsthoorn 2010). In Australië kondigde de politie een onderzoek aan naar de praktijk van Google om in het kader van de Google-internetapplicatie Streetview privé-informatie van draadloze netwerken op te slaan (Trouw 2010). Facebook ligt onder vuur, omdat het bedrijf met de regelmaat van de klok de privacyinstellingen wijzigt, waardoor *default-settings* steeds meer zijn ingericht op het openbaar maken van informatie over de gebrui-

ker, in plaats van het beheren van deze informatie door de gebruiker zelf. Mede onder druk van rechtszaken en slechte pers draaiden deze internetpioniers bepaalde privacyveranderingen terug. Maar voor gebruikers blijft het moeilijk, zo niet onmogelijk, te achterhalen welke sporen ze achterlaten en wat daar vervolgens precies mee wordt gedaan.

1.4 OPZET VAN HET RAPPORT

Tegen de achtergrond van de zojuist geschetste ontwikkeling van de informatiesamenleving wil dit rapport een perspectief ontwikkelen op een zelfbewuste informatieoverheid oftewel iOverheid. Maar ICT en digitalisering zijn voor de WRR geen nieuwe thema's. Waar eerdere rapporten van de WRR zoals *Staat zonder land* (1998) en *Van oude en nieuwe kennis* (2002), nog een verkennend karakter hadden, is er nu meer zicht op de uitwerking van de ontwikkelingen die in die rapporten werden aangekondigd. *Staat zonder land* presenteerde een inventarisatie van toepassingmogelijkheden van ICT, waarvan destijds werd gezegd dat er veel "nog in de kinderschoenen staan" (WRR 1998: 33). Ten tijde van dat rapport had 8 procent van de Nederlanders beschikking over een mobiele telefoon en werd de verwachting uitgesproken dat dit percentage zou toenemen (WRR 1998: 20). Deze verwachting is niet alleen uitgekomen (in 2009 waren er in ons land 125 mobiele telefoonaansluitingen per 100 inwoners (TNO 2009)), maar heeft door een enorme uitbreiding van functies en applicaties een grote en onverwachte dynamiek gekregen. De mobiele telefoon is er niet alleen meer om mee te bellen, maar ook om te e-mailen, twitteren, bestanden uit te wisselen, tv-programma's te bekijken, foto's te nemen en verzenden, een route uit te stippelen, of parkeergeld te betalen. Waar het in voorgaande rapporten nog ging om te verwachten toekomstige ontwikkelingen, groeien jongeren nu op als *digital natives*, niet beter wetend dan met de rest van de wereld verbonden te zijn via het *world wide web* en de mobiele telefoon (Palfrey & Gasser 2008). Deze welhaast alledaagsheid van de vergaande digitalisering van onze samenleving laat ook de overheid niet ongemoeid en heeft, zoals deel II van dit rapport laat zien, ook de bakens voor de overheid sterk verzet.

Wie het discours over digitalisering anno 2011 overziet, moet vaststellen dat deze wordt gedomineerd door bijdragen in twee (conflicterende) toonsoorten. Enerzijds onderbouwen beleidsplannen, rapporten en Kamerstukken de nieuwe mogelijkheden en ambities van de overheid met enthousiaste en wervende uiteenzettingen over de kansen die digitalisering biedt: een veilige samenleving waarin maatschappelijke risico's tijdig in beeld komen; een efficiëntere overheid die zich kenmerkt door dienstverlening op maat aan burgers en die openstaat voor de kennis en kunde van diezelfde burgers. Anderzijds is het debat, met name in wetenschappelijke en maatschappelijke fora, vaak ook negatief van toonzetting. Het gaat over aantasting van de privacy van burgers, verloren miljoenen door mislukte ICT-projecten, niet gerealiseerde verwachtingen, nieuwe kwetsbaarhe-

den als identiteitsfraude en onvoldoende aandacht voor beveiliging van systemen en informatie. Voor- en tegenstanders buitelen over elkaar heen in de rapporten, beleidsdocumenten, nationale en internationale wetenschappelijke literatuur. Wat daarbij opvalt is dat de ontwikkelingen veelal de maat genomen wordt vanuit één specifieke invalshoek (verkleinen van de kloof tussen overheid en burger met interactieve besluitvorming, verhogen van veiligheid, risico's voor privacy en beveiliging, enz.). Bovendien gaan veel opvattingen uit van de vaak onuitgesproken veronderstelling dat de digitaliseringsinitiatieven van de overheid worden ontwikkeld vanuit één consistente visie, gehanteerd door de overheid. In werkelijkheid is dat niet het geval. De digitaliseringsprojecten en initiatieven van de overheid komen niet voort uit een *grand design*. ICT-projecten van de overheid zijn vrijwel per definitie het speelveld voor een conglomeraat aan publieke en private actoren, variërend van diverse overheden, ontwikkelaars, consultants, gebruikers en burgers. Ieder voor zich oefenen ze invloed uit op het eindresultaat. Bovendien gaan informatietechnologische toepassingen gepaard met niet alleen voorziene, maar ook onvoorziene gevolgen in de praktische uitwerking, in de verhouding tussen verschillende betrokkenen en in de verantwoordelijkheidsverdeling.

Om het bestaande discours te overstijgen wordt in dit rapport de bredere dynamiek rondom informatie en technologie voor de relatie overheid-burger in beeld gebracht. De empirische analyse gepresenteerd in deel II is afgebakend door een aantal keuzes. In het kort impliceren deze keuzes dat dit rapport zich richt op (1) informatie als leidend boven technologie, (2) de relatie tussen overheid en burger, (3) een empirische analyse van de bij informatie en technologie betrokken actoren, (4) de dynamiek van beginselen als veiligheid, privacy en transparantie die de discussie en de ontwikkeling van de digitaliseringsinitiatieven sturen en, in aanbevelende zin, (5) de rol en verantwoordelijkheid van de overheid. Deze keuzes worden hier kort toegelicht, vooruitlopend op een verdere uitwerking in hoofdstuk 2.

Het eerste punt houdt in dat dit rapport zich niet richt op de technologische ontwikkelingen *an sich*, maar bovenal inzicht wil bieden in het proces van informatisering (Van de Donk 1997: 153). De aandacht gaat uit naar informatieprocessen die onder invloed van moderne technologie sterk van aard, reikwijdte en effect wijzigen, zijn gewijzigd of mogelijk zullen wijzigen. Nieuwe ICT-toepassingen en technologieën zoals biometrie en RFID-chips zijn dus niet in zichzelf van belang voor dit rapport, maar komen primair in beeld vanuit de invloed die ze hebben op de processen van het creëren, verzamelen en verwerken van informatie.
Ten tweede staat in de analyse de relatie tussen de overheid en haar burgers centraal. Het redeneren vanuit de relatie overheid-burger betekent echter niet dat andere relaties, zoals die tussen overheid en ontwikkelaars, tussen bedrijven en consumenten of tussen burgers onderling geheel buiten beeld blijven. Voor zover ze de inzet van technologie en informatie in de relatie overheid-burger mede bepalen en veranderen, vormen ze onderdeel van de analyse. Beide polen van de as

overheid-burger kennen natuurlijk hun variëteit. 'De' burger en 'de' overheid zijn niet meer dan constructen die het mogelijk maken te redeneren over burgers of overheden in verhouding tot elkaar en andere actoren. In de empirische analyse valt de overheid uiteraard uiteen in diverse overheidsonderdelen en (semi)publieke organisaties en 'de' burger passeert de revue in verschillende rollen en hoedanigheden, zoals patiënt, verzekerde, (probleem)jongere en ouder.
In de derde plaats wordt, om inzicht te krijgen in de processen van digitalisering die de relatie overheid-burger raken, de dynamiek tussen de actoren die betrokken zijn bij digitalisering in beeld gebracht. In empirische zin wordt (ook) voorbij de papieren werkelijkheid van wetgeving en beleidsdocumenten gekeken. De relatie tussen overheid en burger wordt vormgegeven in de dagelijkse praktijk van de ontwikkeling van initiatieven zoals het biometrisch paspoort, het EPD en de plannen en databanken die in Europa worden geïnitieerd. De actoren die daarbij betrokken zijn – van beleidsmakers en politici, via consultants en ontwikkelaars tot eindgebruikers – bepalen gezamenlijk de digitaliseringagenda en de uitkomst daarvan, maar zijn tegelijkertijd zelden zelf onderwerp van onderzoek.
In de vierde plaats komt vanuit de gekozen empirische onderzoeksstrategie aan de orde hoe de verschillende waarden die strijden om voorrang – onder andere, maar niet alleen privacy en veiligheid – ten opzichte van elkaar worden gewogen. Welke rol spelen ze in ontwikkelingstrajecten, en welke actoren maken zich sterk voor welke fundamentele belangen, en met welke argumenten. Daarbij speelt ook dat de politiek-maatschappelijke invulling van deze principes in de loop der tijd door nieuwe omstandigheden, opvattingen en mogelijkheden kan verschuiven.
Ten slotte doet dit rapport aanbevelingen over de verantwoordelijkheden van de overheid tegen de achtergrond van de digitalisering van de samenleving en de overheid zelf. Omdat de technologie niet allesbepalend is, en overheden, ontwikkelaars, gebruikers en burgers mede bepalen óf en hoe bepaalde technologieën een rol gaan spelen, kan de vraag naar eigen, specifieke verantwoordelijkheden van verschillende actoren gesteld worden. Dit rapport richt zich in het bijzonder op de rol en verantwoordelijkheid van de overheid in een informatiesamenleving. Daarbij gaat het in eerste instantie om de verantwoordelijkheid van de overheid als zij zelf gebruikmaakt van ICT in de uitvoering van beleid. Hoe verandert de verantwoordelijkheid van de overheid door het gebruik van ICT en hoe kan die verantwoordelijkheid – in het bijzonder in relatie tot burgers – institutioneel worden vormgegeven?

1.5 AANPAK EN OPBOUW VAN HET RAPPORT

Dit rapport is geschreven op basis van verschillende bronnen. Naast de nationale en internationale wetenschappelijke literatuur heeft de WRR ook twee lijnen van eigen onderzoek uitgezet. De eerste daarvan betreft de vele gesprekken met deskundigen, beleidsmakers en uitvoerders, die van onschatbare waarde zijn geweest voor de totstandkoming van dit rapport. De tweede is het onderzoek dat de WRR ten behoeve van dit rapport heeft uitgevoerd en laten uitvoeren. Er is een

groot aantal essays en empirische studies vervaardigd die in verschillende publicatievormen (als webpublicatie of als hoofdstuk in de WRR-verkenning *De staat van informatie*) beschikbaar zijn gemaakt. Al deze bronnen vormen de bouwstenen voor dit rapport. Ook werd – mede ter toetsing van de aanbevelingen – een aantal discussiebijeenkomsten georganiseerd, waaronder met de Raad van State, de Eerste Kamer en diverse burgerrechtenbewegingen, en is met internationale wetenschappers van gedachten gewisseld tijdens een door de WRR en het Oxford Internet Institute (Oxford, VK) georganiseerd expertseminar.

De aanpak van het onderzoek is sterk empirisch geweest. Het resultaat daarvan is in hoofdzaak terug te vinden in de verschillende deelstudies die zijn gepubliceerd. Dit rapport bevat geen direct verslag van die empirische studies, maar bouwt een redenering op aan de hand van het verzamelde materiaal en de overige bronnen. De empirische hoofdstukken in deel II van dit rapport zijn kortom geen *case studies*, maar trekken verschillende lijnen door het in de onderliggende studies verzamelde materiaal, waarbij de inzichten uit die studies veelvuldig aan bod komen. De empirische studies die voor dit rapport zijn uitgevoerd vallen uiteen in a) domeinstudies, die ontwikkelingen schetsen op een breder (beleids)terrein, en b) black boxen, waarbij op een veel specifieker gebied of naar een concrete toepassing binnen dit terrein onderzoek is gedaan. De inzet voor de black box-studies komt voort uit de wens om de dynamiek rondom informatie en technologie die zich afspeelt tussen de diverse actoren die bij de ontwikkeling van technologische toepassingen betrokken zijn, in kaart te brengen. Veel van die cruciale keuzes en interacties blijven nu voor het brede publiek verborgen en zijn slechts zeer beperkt terug te vinden in de (wetenschappelijke) literatuur. Door het in kaart brengen van de netwerken van systeemontwerpers, bestuurders, instituties en gebruikers rondom technologische toepassingen zoals het biometrisch paspoort, het Elektronisch Patiëntendossier of de Verwijsindex Risicojongeren ontstaat meer zicht op de betekenis van de dynamiek rondom deze toepassing voor de relatie tussen overheid en burgers. Juist omdat het black box-onderzoek dat voor dit rapport is verricht sterk gericht is op het in kaart brengen van de empirische ontwikkelingen, is het daarom ook relatief ‘theoriearm’. George en Bennet (2004: 74) zouden van *atheoretical case studies* spreken: casusmateriaal dat goede, gedetailleerde beschrijvingen biedt die op zichzelf geen bijdrage aan de theorievorming leveren, maar die als input fungeren voor ander, meer meta- en theoretisch gericht, onderzoek.

Bij de selectie van domeinstudies en black boxen is gekozen voor spreiding over de diverse voor dit onderzoek relevante aspecten en invalshoeken. Allereerst komt de burger in verschillende rollen aan bod: als reiziger, patiënt, automobilist en inwoner van een gemeente. Ook de overheid toont zich in de empirische studies in verschillende hoedanigheden: als initiërende kracht van een nieuwe toepassing, als partij in een publiek-private samenwerking, of als wetgever en toezichthouder. Daarbij komen ook de variëteit aan niveaus binnen de overheid (internationaal,

Europees, nationaal en lokaal) en de op deze niveaus gearticuleerde belangen, voorkeuren en onderlinge relaties in beeld. De applicaties en technologieën die nader worden onderzocht hebben allemaal een betekenis voor het genereren, gebruiken, delen en verrijken van informatie, maar wel vanuit verschillende invalshoeken en met onderscheidende doelstellingen. ICT heeft zich inmiddels verspreid over alle sectoren en lagen van de overheid; het is een verhaal van vele actoren, vele rollen, en veel verschillende beleidscontexten.

Bovendien is ter voorbereiding van dit rapport een aantal essays over de bredere en/of conceptuele thema's van het onderzoeksdomein geschreven. Onder meer over overheidsverantwoordelijkheid in het informatietijdperk, afwegingen rondom risico's van informatietechnologie, het recht op vergeten binnen een gedigitaliseerde strafrechtketen en systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechtenverplichting. Ten slotte is in samenwerking met ECP-EPN en Centerdata (Universiteit Tilburg) in week 25 van 2010 een vragenlijst voorgelegd aan 2357 panelleden, van wie 1485 (63%) de vragenlijst volledig hebben ingevuld. Het panel vormt een representatieve steekproef uit de Nederlandse bevolking. Alle onderliggende studies en essays hebben een plaats gekregen in de tegelijk met dit rapport uitgebrachte WRR-verkenning *De staat van informatie* of zijn terug te vinden als webpublicaties op de website van de WRR. In de onderstaande box is een overzicht opgenomen van alle studies met een korte omschrijving.

Box 1.2 Essays, verkenningen en webpublicaties

Essays en verkenningen

De Hert (2011) *Systeemverantwoordelijkheid voor de Informatiemaatschappij als positieve mensenrechtenverplichting*
Deze studie analyseert vanuit mensenrechtelijk perspectief welke verantwoordelijkheden de overheid draagt voor veilige en betrouwbare informatiestromen in onze samenleving.

Meijer (2011) *Overheidsverantwoordelijkheid in het informatietijdperk: een pleidooi voor het creëren van genormeerde experimenteerruimte*
Zowel het gebruik als het niet-gebruik van nieuwe technologieën leidt tot risico's, onzekerheden en problemen rondom overheidsverantwoordelijkheden. Deze studie analyseert ICT-ontwikkelingen bij de overheid en beziet hoe de overheid om kan gaan met nieuwe verdelingen van verantwoordelijkheden.

Van Eeten (2011) *Gedijen bij onveiligheid. Afwegingen rond de risico's van informatietechnologie*
Aan de ene kant is ICT inherent onveilig. Anderzijds wordt onveiligheid en de risico's die daarmee gepaard gaan in de huidige risicomaatschappij niet als iets vanzelfsprekends aanvaard. In dit essay staat de vraag centraal wie de risico's draagt en hoe de kosten en baten van de onveiligheid van

informatietechnologie kunnen worden toebedeeld: welke actoren kunnen de afwegingen rond (on)veiligheid van systemen het beste maken?

Buruma (2011) *Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld*
Digitalisering heeft een enorm virtueel geheugen gecreëerd waardoor vergeten niet meer vanzelfsprekend is. Er worden digitale dossiers aangelegd, DNA-gegevens worden opgeslagen in een database, en allerlei informatie zwerft voor eeuwig over het internet. De vraag of deze ontwikkeling de noodzaak van een recht op vergetelheid rechtvaardigt en of de overheid hierin een rol zou moeten spelen, vormt de kern van deze bijdrage.

Broeders (2011) *Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa*
De rol van technologie aan de grenzen van de EU wordt steeds dominanter. In deze bijdrage wordt de digitalisering van de Europese grenzen geanalyseerd vanuit het perspectief van *surveillance* en het spanningsveld tussen vrijheid en veiligheid. De focus van 'problematische' groepen, als asielzoekers, is inmiddels verbreed naar de *surveillance* en controle van alle reizigers.

Keymolen & Prins (2011) *Jeugdzorg via systemen. De Verwijsindex Risicojongeren als spin in een digitaal vangnet*
Aan de hand van de Verwijsindex Risicojongeren wordt in deze bijdrage geanalyseerd hoe in het domein van de jeugdzorg ICT wordt ingezet om ambities als vroegtijdig en proactief ingrijpen mogelijk te maken. Hierbij worden zowel de ontwikkelingen op rijksniveau als op lokaal niveau onder de loep genomen.

Keizer (2011) *De digitale patiënt centraal. Medische informatie in een digitale wereld*
In deze studie wordt een analyse gemaakt van de betekenis van digitalisering van medische informatie voor de bestaande relaties binnen dit domein. De verhouding tussen overheid en burger wordt in ogenschouw genomen, maar ook de relatie tussen behandelaars en patiënten, alsmede de onderlinge verhoudingen tussen intermediërende actoren zoals zorginstellingen en artsen.

Snijders (2011) *Chief Information Officers bij de Rijksoverheid*
Chief Information Officers (CIO's) zijn bij de rijksoverheid aangesteld ter verbetering van de positionering en kwaliteit van het informatiemanagement. In deze bijdrage wordt nader inzicht verschaft in de heersende opvattingen over de aanstelling, de te leveren bijdrage en de taken en bevoegdheden van de CIO.

Choenni, Leertouwer & Busker (2011) *Klachten over toepassingen van informatietechnologie. Analyse van een aantal overheidsbestanden*
In deze bijdrage wordt inzicht verkregen in de relatie overheid-burger door het in kaart brengen van klachten van burgers over de ICT-applicaties van de overheid. Deze bijdrage analyseert hiertoe een aantal bestanden van overheidsinstanties die belast zijn met het afhandelen van klachten van burgers.

Alle essays en verkenningen zijn gepubliceerd in D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.) (2011) *De staat van informatie*, WRR-verkenning 25, Amsterdam: Amsterdam University Press.

Webpublicaties

Pluut (2010) *Het landelijk EPD als black box. Besluitvorming en opinies in kaart*
De diverse *stakeholders,* betrokken bij het landelijk Elektronisch Patiëntendossier (EPD), beoordelen de gevolgen van dit dossier voor zaken als de kwaliteit van zorg, efficiëntie, privacy en aansprakelijkheid zeer verschillend. Deze bijdrage brengt het besluitvormingsproces en het krachtenveld rondom het landelijke EPD in kaart.

Böhre (2010) *Happy Landings? Het biometrische paspoort als zwarte doos*
Doel van dit onderzoek is om enig licht te werpen op het biometrische paspoort als maatschappelijk-technologische black box en op de politieke en maatschappelijke dynamiek die daarbinnen (en ook daaromheen) tot nu toe is opgetreden.

Van Loon (2010) *Goed opdrachtgeverschap jegens ICT Uitvoeringsorganisatie (ICTU)*
ICTU kan namens verschillende onderdelen van de Nederlandse overheid optreden als tussenschakel naar de markt toe bij de ontwikkeling van ICT-voorzieningen. Hiertoe worden haar opdrachten verstrekt door uiteenlopende overheidsinstanties. De kwaliteit van het opdrachtgeverschap van deze instanties vormt het zwaartepunt van dit onderzoek.

Attema & De Nood (2010) *Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit*
In dit survey-onderzoek (dat ECP-EPN in samenwerking met de WRR heeft uitgevoerd) staan de rol en verantwoordelijkheid van de overheid bij de inzet van ICT centraal. Het onderzoek richt zich op de consequenties van de inzet van ICT voor de relatie overheid-burger en op de betekenis van deze consequenties vanuit de verantwoordelijkheid van de overheid wanneer ze ICT inzet in bedrijfsvoering, beleid en beleidsuitvoering.

Holvast & Bonthuis (2010) *Black box-onderzoek Veiligheidshuizen*
In deze bijdrage worden de beleidsopvattingen en afwegingen die gemaakt zijn bij het opzetten van Veiligheidshuizen geanalyseerd. Een Veiligheidshuis is een stedelijk kantoor waar, in een samenwerkingsverband van politie, justitie en gemeente, de volledige coördinatie plaatsvindt van de aanpak van jongeren die met politie en justitie in aanraking komen.

Potters & De Vreeze (2010) *eCall Black Box*
Deze bijdrage analyseert eCall, het Europese initiatief waarbij auto's worden voorzien van elektronica die een geautomatiseerde of handmatige noodoproep uitzendt in geval van een ongeluk. In deze noodoproep kunnen diverse gegevens over bestuurder en passagiers worden meegezonden.

Snijder (2010) *Het biometrische paspoort in Nederland: crash of zachte landing*
Deze studie analyseert vanuit de techniek, de industrie en de politiek de totstandkoming van het Nederlandse biometrisch paspoort. De analyse biedt inzicht in mogelijke gevolgen (op de lange termijn) voor burgers in hun relatie met de overheid en hoe deze in het besluitvormingsproces van de nieuwe Paspoortwet zijn meegenomen.

Griffioen (2011) *'Location based privacy' in constellaties van publiek-private verantwoordelijkheid*
Deze studie gaat in op het gegeven van locatie als een onderdeel van privacy. Wat betekent de traceerbaarheid van individuen in het (openbaar) vervoer voor de privacy van burgers, en hoe komt deze in verschillende varianten van publiek-private samenwerking tot zijn recht?

Dit rapport is als volgt opgebouwd. Het bestaat uit drie delen en bevat negen hoofdstukken en een epiloog. *Deel I, inleiding en onderzoekskader*, omvat behalve dit inleidende hoofdstuk ook hoofdstuk 2, waarin een aantal theoretische uitgangspunten en concepten worden uitgewerkt als gereedschap voor de analyse van het empirische materiaal. In *Deel II, de empirische analyse*, wordt de digitalisering van de overheid in een vijftal hoofdstukken in kaart gebracht en geanalyseerd. De analyse is in hoofdzaak opgezet aan de hand van de ontwikkelingen, rol en interacties van de voornaamste actoren in het digitale overheidsdomein. Hoofdstuk 3 richt zich daarbij op de politiek. De dynamiek binnen de overheid, zowel tussen 'Den Haag' en uitvoeringsinstellingen als tussen 'Den Haag' en lagere overheden, staat centraal in hoofdstuk 4. Hoofdstuk 5 verlegt de blik naar het internationale en Europese niveau. De verhouding tussen overheden en verschillende marktpartijen, waaronder de nieuwe grote spelers van de informatiesamenleving en bedrijven die de applicaties voor de overheid ontwikkelen en maken, vormt het onderwerp van hoofdstuk 6. Hoofdstuk 7 richt zich allereerst op een aantal (overheids)instituties die op verschillende manieren een vorm van toezicht of controle uitoefenen op de ontwikkeling van de iOverheid en een rol hebben als *countervailing power*. Vervolgens besteedt dit hoofdstuk ook aandacht aan de rol die burgers als digitale tegenkracht spelen. *Deel III, analyse en aanbevelingen*, maakt de balans van het empirische onderzoek op. Hoofdstuk 8 bepleit een wisseling van het paradigma waarmee de overheid digitalisering tegemoet treedt. Het nog altijd dominante idee van de eOverheid moet vervangen worden door dat van de iOverheid. Hoofdstuk 9 werkt die paradigmawisseling uit in inhoudelijke, procedurele en institutionele aanbevelingen die het besef 'een iOverheid te zijn' stevig in niet alleen het doen en laten, maar ook de organisatie en het denken van de overheid moet verankeren. De epiloog, ten slotte, schetst de contouren van de bredere verantwoordelijkheid van de overheid tegen de achtergrond van de snelle ontwikkelingen in de iSamenleving.

NOTEN

1 In opdracht van president Obama is in december 2009 de Open Government Directive opgesteld die departementen en agentschappen instrueert om specifieke maatregelen door te voeren die een 'open overheid' ondersteunen. De basis voor deze open overheid vormen de principes transparantie, participatie en samenwerking. Onderdeel van de maatregelen is dat zonder tegenindicatie informatie van departementen en agentschappen altijd openbaar moet zijn. (http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf)

2 De Britse overheid heeft duizenden datasets openbaar gemaakt op de website www.data.gov.uk. Zowel individuele burgers, als organisaties en ontwikkelaars kunnen de datasets doorzoeken, maar daarnaast ook informatie kopiëren en hergebruiken. De website bevat ook een wiki waarop informatie kan worden gedeeld over gebruikte technieken om de data verder te verwerken.

3 "Het kabinet wil transparant zijn over het wetgevingsproces en wil de in de samenleving aanwezige kennis beter benutten bij de voorbereiding van wetgeving. Daarom informeert de overheid met ingang van 24 juni 2009 burgers, bedrijven en maatschappelijke organisatie via internet over voorgenomen wetgeving. Daarnaast biedt zij de gelegenheid om via internet ideeën en suggesties te doen voor nieuwe wetgeving. Het gaat om een rijksbreed experiment met een looptijd van twee jaar." (internetconsultatie.nl, geraadpleegd op 3 november 2010).

4 Ten opzichte van de voorloper *Naar een veiliger samenleving* onderscheidt het kabinetsprogramma *Veiligheid begint met voorkomen* van het kabinet Balkenende-IV zich door nadrukkelijk te kiezen voor een combinatie van preventie, bestuurlijke en strafrechtelijke handhaving en nazorg (Tweede Kamer 2007-2008b).

5 Interview dhr. M. van Asperdt, hoofd afdeling Expertise en Innovatie Nationaal Bureau voor Verbindingsbeveiliging (NBV), juli 2010; interview dhr. B. Jacobs, hoogleraar RU, juni 2010.

2 ANALYTISCH KADER: INFORMATIE, ACTOREN EN BEGINSELEN

Het is ontelbare malen gezegd en geschreven: digitalisering heeft een ongekende invloed op ons doen en laten, op onze samenleving. De tientallen rapporten die de afgelopen jaren over ICT zijn verschenen, hanteren stuk voor stuk kwalificaties als *revolutionaire* ontwikkelingen, *unieke* kansen, *complexe* spanningen, *fundamentele* veranderingen, *schuivende* belangen en *verouderde* sociale en institutionele kaders. Maar waarin exact schuilt die ongekende invloed van digitalisering? Waarom precies zijn de kansen, spanningen, verschuivingen en uitdagingen te duiden als fundamenteel, uniek of complex? En wat zijn dan die gevolgen van digitalisering wanneer specifiek de relatie tussen overheid en burgers in ogenschouw wordt genomen? Wie de kwalificaties terzijde schuift en op zoek gaat naar de kenmerken die ICT 'anders' dan wel 'nieuw' maken, stelt vast dat digitalisering een minder eenduidige ontwikkeling is dan op het eerste gezicht lijkt. Hoewel 'digitalisering' een omlijnd en helder fenomeen lijkt te suggereren, wordt ze in de praktijk van alledag gevormd door een diversiteit van ontwikkelingen, technologische doorbraken en specifieke applicaties. Op hun beurt worden deze ontwikkelingen, doorbraken en applicaties geïnitieerd en in de loop der tijd gestuurd door een veelheid aan actoren, hun interacties en de voorziene en onvoorziene gevolgen die deze interacties met zich meebrengen. De volgende hoofdstukken (van deel II) beogen deze dynamiek van actoren, processen en belangen inzichtelijk te maken, waarbij de analyse zich specifiek richt op de relatie tussen overheid en burger(s). Aan de hand van de geschetste empirische werkelijkheid wordt meer zicht verkregen op de gevolgen van digitalisering voor deze specifieke relatie. Maar alvorens deze werkelijkheid in beeld te brengen, biedt dit tweede hoofdstuk daartoe het analysekader. Hiernaast presenteert het een nadere uitwerking van de centrale thema's en kernbegrippen die in het rapport centraal zullen staan.

Zoals gezegd, richt de analyse in dit rapport zich niet zozeer op de ontwikkeling van individuele technologieën, maar op de vraag hoe die technologieën een rol spelen in de relatie tussen verschillende actoren. Dit rapport kiest kortom voor de bestudering van het 'sociotechnologisch complex' en gaat vanuit dit perspectief in op de wisselwerking tussen technologie en informatie (par. 2.2). Na deze plaatsbepaling biedt dit hoofdstuk een descriptief en normatief kader dat richting geeft bij het in kaart brengen van de empirische werkelijkheid. Daarbij ligt de nadruk op de praktische ontwikkelingen en reële verplaatsing in termen van positie, gezag en invloed van de verschillende actoren. Daartoe geeft paragraaf 2.3 allereerst een schets van die centrale actoren: overheid, burgers en de technologische applicaties. Om de dynamiek van de empirische werkelijkheid te duiden wordt vervolgens in paragraaf 2.4 een normatief kader geïntroduceerd. Door middel van een driedeling in stuwende, verankerende en procesmatige beginselen wordt de diversiteit en

veelkleurigheid aan concrete beginselen (variërend van efficiëntie via transparantie tot keuzevrijheid) die telkens terugkeren in beleidsvoorstellen en publieke en politieke debatten, in kaart gebracht. De dynamiek tussen deze drie soorten beginselen, is een belangrijk normatief-analytisch instrument om de empirische ontwikkelingen die in deel II aan bod komen, te duiden en verklaren.

2.1 PERSPECTIEVEN OP DE RELATIE TUSSEN TECHNOLOGIE EN HAAR GEBRUIKERS

In dit rapport staat de vraag naar de consequenties van de inzet van ICT in de relatie overheid-burger(s) centraal. Wie deze vraag wil beantwoorden moet allereerst duidelijk maken hoe precies de rol en invloed van technologie wordt geduid. Is technologie, of dat nu een OV-chipkaart, biometrie of beveiligingscamera is, niets anders dan een neutraal instrument in handen van politici, beleidsmakers en burgers? Of is het juist een onomkeerbare kracht die zich volgens een eigen logica ontplooit en daarmee eigenstandig een grote invloed heeft? Het antwoord op deze vragen raakt aan een academisch debat over de conceptuele duiding van technologie en de verschillende zwaartepunten die men kan leggen in het onderzoek naar technologie, samenleving en de interactie daartussen. In de literatuur is hierover een veelheid aan perspectieven en nuanceringen te vinden. Alhoewel de hierna te hanteren positionering niet ten volle recht doet aan de rijkdom van het wetenschappelijk debat over het karakter en de plaats van technologie in de samenleving, vallen de perspectieven zoals ze in het publieke debat en de politiek-bestuurlijke realiteit worden gehanteerd grosso modo in drie grote groepen uiteen. Aan de ene zijde van het spectrum staat een instrumenteel en aan de andere zijde van het spectrum een technologisch deterministisch perspectief. In het middengebied bevindt zich een druk multidisciplinair veld dat er een meer constructivistische benadering op na houdt. Door de actoren – burger(s), overheid en 'applicaties' – in dit onderzoek centraal te stellen en de interactie tussen sociale en technologische invloeden te onderzoeken, wordt al direct duidelijk dat dit onderzoek zich plaatst in dit constructivistische midden. Alvorens nader in te gaan op dit middengebied, schetst het onderstaande allereerst meer algemeen het bredere spectrum van perspectieven. Meer of minder expliciet worden, zoals opgemerkt, immers alle drie de perspectieven in het publieke debat gehanteerd.

2.1.1 HET SPECTRUM VAN INSTRUMENTALISME TOT TECHNOLOGISCH DETERMINISME

In het *instrumentalisme* is techniek een neutraal en waardevrij middel dat op verschillende manieren kan worden ingezet. Technologische applicaties zijn de neutrale dragers van de ideeën en doelstellingen van de ontwerpers. Maatschappelijke ontwikkelingen zijn autonoom en sturend voor de technologische ontwikkelingen. Technologie leent zich in deze visie dan ook uitstekend als *problem solver*

Box 2.1 Burgerservicenummer (bsn): neutraal instrument of kracht met eigen logica?

Tijdens de parlementaire behandeling van het wetsvoorstel Burgerservicenummer (BSN) werd door de minister benadrukt dat dit unieke persoonsnummer niet meer is dan een informatieloos nummer, daarmee suggererend dat het neutraal in uitwerking en effecten is. VNO-NCW verwoordde deze opvatting expliciet: "Als algemeen commentaar kan gesteld worden dat het BSN in zich geen risico's oplevert. Het nummer is neutraal. Uitwisseling die zonder BSN niet is toegestaan zal dat met BSN evenmin zijn" (Inbreng VNO-NCW in BSN-discussie bij College Bescherming Persoonsgegevens, 30 januari 2006). Vanuit verschillende fracties in Tweede en Eerste Kamer werd echter opgemerkt dat het nummer de "toenemende informatiemacht van de overheid" faciliteert (Tweede Kamer 2005-2006c: 1). Ook werd de zorg geuit dat met de beschikbaarheid van het BSN, organisaties in niet alleen de publieke maar ook in de private sector, hun werkwijzen en informatiebehoeften zouden gaan aanpassen (Eerste Kamer 2007-2008). Inmiddels laten diverse voorbeelden zien dat het BSN kennelijk meer is dan een neutraal instrument en zich ontwikkelt tot een aantrekkelijk beleidsvehikel. Zo is een wetsvoorstel in voorbereiding voor het gebruik van het BSN in de financiële sector (Eerste Kamer 2009-2010f), ontstond zomer 2010 een felle discussie tussen het College Bescherming Persoonsgegevens en het ministerie van Verkeer & Waterstaat over het gebruik van het BSN op de Rijkspas (CBP 2010a) en wordt bij het ministerie van EZ onderzocht in hoeverre het nummer gebruikt kan worden in het kader van de elektronische herkenning (eHerkenning) van bedrijven en zelfstandigen zonder personeel bij digitale dienstverlening (Leenes, Koops & Van der Wees 2010). De staatssecretaris van BZK liet eind augustus 2010 weten vooralsnog geen aanleiding te zien tot het opstellen van een overkoepelend beoordelingskader voor het (bredere) gebruik van het BSN (Eerste Kamer 2009-2010f). Ruim twee jaar daarvoor had het parlement de regering verzocht aan te geven welk beoordelingskader gerealiseerd kon worden (Eerste Kamer 2007-2008).

voor tal van moeilijkheden, het is een instrument dat vrij inzetbaar is (Kaplan 2009: xvi). In het politieke domein leidt dit ertoe dat men gemakkelijk naar technologische mogelijkheden grijpt om – maatschappelijke – problemen op te lossen (zie ook Van den Berg et al. 2008). Dat wil overigens niet zeggen dat men ervan overtuigd is dat het gebruik van technologie altijd tot goede uitkomsten leidt. Wanneer de resultaten van de technologische oplossingen tegenvallen, zijn het de gebruikers die hiervoor verantwoordelijk zijn en niet de technologie (Van de Donk & Depla 1993). Technologie is immers waardevrij en slechts een 'instrument' in de handen van personen die het ten goede en ten kwade kunnen inzetten. Hoewel de idee van technologie als een neutraal instrument in academische kringen de laatste decennia aan belang heeft ingeboet, is de gedachte binnen de overheid vaak nog zeer levendig, aldus recente rapporten van de Algemene Rekenkamer (Algemene Rekenkamer 2007a; Edge 1995; MacKenzie 1999a: 43).

Het *technologisch determinisme* gaat uit van de centrale aanname dat technologie de maatschappij in belangrijke mate vormgeeft. Technologie wordt voorgesteld als

een onomkeerbare kracht die zich volgens een eigen logica ontplooit en een grote invloed heeft op de wijze waarop werk, economie en de maatschappij als geheel ingericht zijn (Williams & Edge 1996: 55). Frissen concludeerde in 1996 al dat de instrumentele positie van technologie die in het moderne beheersingsstreven verondersteld wordt, nauwelijks meer kan worden volgehouden als gevolg van de autonome macht van technologie (Frissen 1996: 344). Van recentere datum is de opmerking van het Tweede Kamerlid Van Raak (SP) tijdens een algemeen overleg over de nationale databank waarin biometrische kenmerken zullen worden opgeslagen.

"De middelen zullen de moraal bepalen. Stel, je hebt zo'n databestand. Er vindt een verschrikkelijk misdrijf plaats. Dan willen politieagenten dat toch oplossen. En als dan de mogelijkheid bestaat ... Het creëren van het databestand zal straks het gebruik creëren. Natuurlijk gaat het databestand in de toekomst gebruikt worden voor allerlei andere zaken. Dat is iets wat de staatssecretaris volgens mij ook best weet" (Tweede Kamer 2010-2011a: 15).

Technologisch determinisme kent verschillende gradaties. Binnen de sterke variant is technologie een voldoende voorwaarde om gedrag te veranderen en zelfs hele maatschappijen te transformeren (Chandler 1996). Binnen de zwakke variant is technologie weliswaar nog steeds de bepalende, maar niet langer de enige factor (MacKenzie 1999b). Binnen het perspectief van technologisch determinisme klinken zowel positieve als negatieve geluiden over technologie. Technologieoptimisten menen dat alles wat technologisch mogelijk is ook gerealiseerd zal worden en de maatschappij ten goede zal komen (Van den Berg 2009: 42). Technologiepessimisten gaan er eveneens van uit dat wat technologisch mogelijk is in de praktijk ook gebracht zal worden, maar spreken hierover in termen van 'overrompeling' en 'verlies van autonomie en solidariteit'. Zij vrezen voor een wereld geleid door een technologische rationaliteit, met weinig oog voor de menselijke maat (Ellul 1954; Ellul 1977; Anders 1980).

Dit rapport positioneert zich, zoals hiervoor al opgemerkt, in het gebied tussen het instrumentalisme en technologisch determinisme. Op deze positie ook vindt een grote variëteit aan onderzoekers uit verschillende intellectuele tradities elkaar in het doel 'de black box van de technologie' te openen (MacKenzie & Wajcman 1985; Bijker & Law 1992; Williams & Edge 1996: 54). In de jaren tachtig en negentig van de vorige eeuw ontwikkelde zich, mede in reactie op het technologisch determinisme en instrumentalisme, een interactief perspectief op technologie met als centrale aanname dat technologie en maatschappij elkaar wederzijds beïnvloeden (Fuglsang 2001). Vanuit deze aanname worden technologie en technologische concepten onderzocht in relatie tot de sociale werkelijkheid en niet als een apart domein (Kaplan 2009). Technologieën zelf zijn zowel oorzaak als gevolg van ontwikkelingen in de maatschappij (Williams & Edge 1996: 55). In dit *constructivistisch* perspectief richt de aandacht zich in het bijzonder op het ontwikkelings-

proces van specifieke technologische applicaties en de rol die de betrokken actoren spelen. De centrale gedachte is dat er keuzemogelijkheden zijn als het gaat om de uiteindelijke vorm die een technologische applicatie aanneemt (Williams 1999: 41). Een technologisch artefact komt niet zomaar tevoorschijn uit het niets. Het wordt geboren uit de sociale, economische en technologische relaties die reeds aanwezig zijn (Bijker & Law 1992). Naast deze aandacht voor de sociale constructie van technologie is er, zeker de laatste jaren, ook aandacht voor de werking van de technologie zelf. Wanneer een technologie eenmaal een stabiele betekenis en plaats heeft verworven in de maatschappij, is het niet eenvoudig meer om veranderingen in die technologie aan te brengen. Betrokkenen hebben in een bepaalde vorm en gebruik van een applicatie geïnvesteerd waardoor deze deel uitmaakt van een netwerk aan praktijken en instituties. Tot op zekere hoogte kan een technologie de sociale ontwikkeling dan als het ware gaan 'bepalen' (Bijker 2001: 28-29). Dit wil echter niet zeggen dat 'volwassen' socio-technologische systemen onstuurbaar zijn, maar wel dat het veel meer inspanning vergt om veranderingen door te voeren.

2.1.2 HET SOCIO-TECHNOLOGISCH COMPLEX ALS ONDERZOEKSOBJECT

Dit onderzoek vertrekt vanuit de gedachte dat sociale relaties technologie vormen en dat technologie tegelijkertijd ook invloed uitoefent op die sociale relaties. De keuze voor dit vertrekpunt komt voort uit de focus op de consequenties van de inzet van ICT voor de relatie overheid-burger. ICT is hierbij een onderdeel van een dynamiek waarin meerdere processen, belangen en actoren samenkomen. Dit complexe netwerk van instituties en technologische toepassingen wordt, in navolging van het constructivistisch perspectief, het socio-technologisch systeem genoemd. Door het in kaart brengen van verschillende socio-technologische systemen rondom ondermeer de Verwijsindex Risicojongeren, het biometrisch paspoort, eCall en het landelijk Elektronisch Patiëntendossier, wordt in deel II scherper in beeld gebracht welke effecten de inzet van ICT heeft in de relatie overheid-burger. Drie aandachtspunten staan in de empirische analyse van deel II centraal.

Het eerste aandachtspunt is de rol van de *actoren*. De manier waarop technologische toepassingen worden ontwikkeld en gebruikt is immers afhankelijk van de belangen, beïnvloedingsmogelijkheden, visies, kennis en vaardigheden, toekomstverwachtingen, waarden en percepties van actoren (zoals ontwikkelaars, bestuurders, gebruikers en niet-gebruikers) en technische mogelijkheden en onmogelijkheden (Stirling 2008). Hierbij is er ook aandacht voor machtsverhoudingen. Welke actoren zijn al dan niet in staat om de ontwikkeling van een technologie te sturen? De strijd die soms woedt over de manier waarop een applicatie ontworpen en gebruikt moet worden, speelt zich niet af op een *level playing field*. De interacties tussen instituties, culturen en systemen kenmerken zich eerder

door verschillen in invloed en macht (Mansell & Silverstone 1996: 213). Zo kan het zijn dat personen die de uiteindelijke technologie gebruiken geen inspraak hebben bij de totstandkoming ervan en dat er actoren zijn die, hoewel ze niet tot de direct betrokkenen behoren, toch beïnvloed worden in hun handelen door de werking van de technologie. Zo zal hoofdstuk 3 onder meer wijzen op de kloof tussen enerzijds beleidsmakers die de opdracht tot de ontwikkeling en uitwerking van een applicatie geven en anderzijds de professionals die op uitvoeringsniveau met de applicatie moeten gaan werken, maar geen stem hebben gehad bij de ontwikkeling daarvan.

Een tweede aandachtspunt in de analyse is de factor *tijd*. Zo benadrukt Hughes (1994) dat in de ontwikkelingsfase van de technologie de invloed van organisaties, groepen en individuen groot is. Naarmate de tijd echter vordert en een applicatie ingebed raakt in de maatschappij, neemt de complexiteit van het systeem toe en neemt de mogelijkheid tot controle over de technologie af. De technologie verkrijgt dan een eigen momentum. Als de technologie eenmaal is ontwikkeld, bepaalde diensten levert en er tijd en geld is gespendeerd, wordt fundamentele bijsturing moeilijker (Hughes 1994). In feite kent de ontwikkeling van technologie drie fases. In de beginfase is er sprake van een grote mate van ‘interpretatieve flexibiliteit’, de technologische applicatie is nog ‘open’ en er zijn nog verschillende betekenissen en keuzes mogelijk. Ontwerpers, opdrachtgevers, overheden, consultants, wetenschappers en (beoogde) gebruikers hebben allerlei ideeën en wensen over hoe de technologische applicatie eruit moet komen te zien. Pinch en Bijker (1984: 414) spreken hier van “relevante sociale groepen” die, al dan niet georganiseerd, invloed uitoefenen op het ontwikkeltraject. Zo laten Keymolen en Prins (2011) in hun studie van de Verwijsindex Risicojongeren (VIR) zien, dat op lokaal niveau systeemontwikkelaars en consultants in de beginfase relatief veel invloed konden uitoefenen op de systeeminrichting op informatieniveau. Wanneer de technologische applicatie in de vervolgfase haar uiteindelijke vorm heeft gekregen, is deze (mede) een reflectie van de relaties, overtuigingen en belangen van bij het ontwerp en de implementatie betrokken actoren (Woolgar 1996: 87-88). In de laatste fase beweegt de applicatie zich in een wijdere maatschappelijke en politieke context en kan op haar beurt ook bepalend worden voor sociale relaties. Of zoals te lezen valt bij Johnson & Wetmore (2009: xiii):

> “Once created, sociotechnical systems can sometimes seem to take on a power of their own. They facilitate and constrain certain actions and thereby facilitate and constrain certain values. In other words, the intertwining of society and technology is not neutral; it is value laden.”

Een laatste zwaartepunt is het *niveau van analyse*. Allereerst wordt gekeken hoe een specifieke technologie zich ontwikkelt en wie daarbij zijn betrokken. Hiernaast geeft de analyse in deel II ook rekenschap van tendensen op macroniveau

zoals economische belangen, internationale wetgeving, globalisering en de roep om veiligheid. Niet in de laatste plaats omdat deze sociaal-maatschappelijke ontwikkelingen van invloed zijn op de actoren, hun belangen en de context waarin een technologie vorm krijgt. Het in kaart brengen van zowel de processen rondom een specifieke technologie als de brede maatschappelijke veranderingen die deze processen raken, maakt dat er een gelaagd beeld ontstaat van de werking van ICT binnen de relatie overheid-burger.

2.2 TECHNOLOGIE EN INFORMATIE

Binnen het begrippenpaar technologie en informatie richt dit onderzoek de aandacht primair op informatie, meer in het bijzonder op de wijze waarop de diversiteit aan actoren het gebruik van informatie beïnvloedt en verandert. Deze 'informationele' kant van ICT staat uiteraard niet los van de technologie. De toepassing van biometrie op het paspoort laat bijvoorbeeld zien dat de inzet van technologie bepalend is voor het soort van informatie dat wordt verzameld dan wel kan worden verzameld. Het is ook de technologie die bepaalde informatiestromen faciliteert dan wel de toegang tot informatie dicteert. Zo ligt het in de gebruikte software vast dat een Elektronisch Patiëntendossier dat wordt beheerd door een individuele zorgverlener, toegankelijk wordt voor andere zorgverleners. Hoe precies een concrete technologie het verzamelen, gebruiken en uitwisselen van informatie vormgeeft kan alleen op het niveau van concrete applicaties en koppelingen worden bestudeerd. In dit rapport ligt de nadruk dan ook niet op dé biometrie of op dé netwerktechnologie (het technologieniveau), maar op het biometrisch paspoort en een digitaal dossier (het applicatieniveau). ICT staat daarbij voor alle technologische applicaties, ook wel toepassingen genoemd, die gebruikt worden om informatie te verzamelen, op te slaan, te verwerken, te verrijken en uit te wisselen.

2.2.1 VAN GEGEVENS EN DATA VIA INFORMATIE NAAR KENNIS

Wie kijkt naar het onderdeel informatie uit het begrippenpaar ziet dat het verschillende verschijningsvormen kent, afhankelijk van het verwerkingsstadium. In eerste instantie worden er data en gegevens verzameld en elektronisch vastgelegd. Data en gegevens zijn betekenisloos. Op het niveau van data en gegevens is immers nog geen sprake van filtering, interpretatie of verwerking. Ze representeren echter al wel een feit. Soms wordt een onderscheid gemaakt tussen data en gegevens, waarbij data niet geordend en gegevens al enigszins geordend zijn. In dit rapport worden beide termen echter als synoniem gebruikt. Door vervolgens alleen die gegevens te beschouwen die relevant zijn binnen een bepaalde context en voor een bepaalde groep van gebruikers ontstaat er informatie. Met andere woorden, wanneer gegevens onderling, vanuit een stelsel, met het oog op een bepaald (beleids)doel worden geordend en met elkaar in verband

worden gebracht ontstaat informatie. Of zoals Liebenau & Backhouse (1990) stellen: "Information is data arranged in a meaningful way for some perceived purpose" (in Canhoto & Backhouse 2008: 48). Het is dus niet zo dat door meer data te verzamelen er automatisch ook meer informatie ontstaat. Sterker nog, een overvloed aan data kan ertoe leiden dat er dusdanig veel 'ruis' op de gegevens zit dat het moeilijk is daar relevante informatie uit te destilleren. Door verschillende informatiecomponenten met elkaar in verband te brengen en toe te passen ontstaat ten slotte kennis. Kennis krijgt voornamelijk waarde wanneer deze gebruikt wordt voor, en aanleiding kan geven tot, actief handelen (Van der Lubbe 2002).

Onze huidige samenleving wordt vaak gekenschetst als informatiemaatschappij (Castells 1996) of kennismaatschappij (WRR 2002). Waar in de loop der eeuwen grond, arbeid en geld zich ontpopten als belangrijke productiefactoren, zijn daar recent informatie en kennis als prominente productiefactoren, als 'kapitaal', aan toegevoegd. Door middel van ICT is het nu mogelijk om snel en goedkoop data te verzamelen, op te slaan, te bewaren en te delen op een ongekende schaal (Mayer-Schönberger 2009). Het is echter belangrijk voor ogen te houden dat informatie altijd al een economische en sociale waarde had. Geen maatschappij kan voortbestaan zonder er op een of andere manier voor te zorgen dat informatie, maar ook kennis, wordt gedeeld en overgedragen (Porter 1995: 45). Of het nu gaat om tradities op basis van spraak of tekens, de boekdrukkunst, film of ICT, het overdragen, filteren en onthouden van informatie is een van de rode draden van de geschiedenis. Zo is informatieverzameling ook altijd een centraal aspect van staatsvorming geweest. De informatieopbouw had overigens ook een emancipatoir karakter. Door elke burger een identiteit te geven bood Napoleon burgers de mogelijkheid zich te emanciperen *vis-à-vis* de aristocratie. Maar het was toch primair de opbouw van de bureaucratische staat die noodzaakte tot het verzamelen, classificeren en opslaan van informatie over burgers. Scott (1998) stelt dat de overheid de samenleving door informatieverzameling 'leesbaar' probeert te maken. Individuele burgers worden in kaart gebracht als belastingbetalers, dienstplichtigen, werknemers enzovoorts (vgl. ook Caplan & Torpey 2001: 1). Die informatie en leesbaarheid zijn fundamenteel voor het vermogen van de staat om de samenleving te kunnen besturen. Auteurs als Weber en Foucault zagen de bureaucratie als een zeer rationeel systeem van informatieverzameling en administratieve controle. Torpey (1998) heeft er bovendien op gewezen dat de mogelijkheden van de staat om in te kunnen grijpen (*penetrate*) in sociale processen afhangt van het vermogen van de staat om die samenleving te kunnen 'omvatten' (*embrace*): "As states grow larger and more administratively adept they can only penetrate society effectively if they embrace society first. Individuals who remain beyond the embrace of the state necessarily represent a limit on its penetration" (Torpey 1998: 244). De neiging van overheden om zoveel mogelijk data te verzamelen – Sheptycki (2007) spreekt van *compulsive data demand* (dwangmatige datavraag) – is groot en lijkt in de huidige informatiemaatschappij zeker niet af te nemen.

2.2.2 HET DRAAIT OM TOEGANG, CONTROLE EN KENNIS

Het belang van informatie als zodanig is echter niet datgene wat onze huidige informatie- en kennismaatschappij zozeer kenmerkt. Twee in het oog springende en in dit rapport centrale kenmerken van de wisselwerking tussen technologie en informatie zijn veeleer 1) de wijze waarop informatie al dan niet toegankelijk wordt gemaakt en 2) de manier waarop informatie wordt geselecteerd en wordt omgezet in kennis.

Het is allereerst de mate waarin en manier waarop informatie al dan niet *toegankelijk* wordt gemaakt die betekenisbepalend lijkt te worden. De kracht van ICT ligt er juist in (nieuwe) informatie zowel toegankelijk te maken als de toegang tot informatie te sturen en te controleren (Dutton 1999: 11-12). Dat het veeleer om toegang en daarmee uitwisseling van informatie gaat, blijkt bijvoorbeeld uit het initiatief voor de Verwijsindex Risicojongeren (VIR). Deze is – om tragische gebeurtenissen als 'het Maasmeisje' te voorkomen – primair in het leven geroepen om de informatie-uitwisseling tussen hulpverleners in de jeugdzorg te verbeteren, in het bijzonder uitwisseling tussen partners die niet van nature met elkaar in contact staan. Waar vroeger informatie werd gedeeld tussen bekenden, biedt ICT nu ook (en soms zelfs vooral) de mogelijkheid communicatie en interactie tot stand te brengen tussen actoren die elkaar niet kennen (Porter 1995: 46). Belangrijk hierbij zijn 1) de koppeling van gegevens, 2) de mogelijkheid gegevens snel en eenvoudig te kopiëren en 3) het feit dat gegevens persisteren (Van den Berg & Leenes 2011).

Individuen en organisaties 'openbaren' en delen steeds meer informatie over zichzelf en anderen, waarbij digitalisering van deze informatie de verspreiding en de koppelbaarheid daarvan, zowel in het publieke als het private domein, eenvoudiger maakt. Informatie migreert bovendien makkelijk van de ene naar de andere context en daarmee staat ook het onderscheid tussen publiek en privaat onder druk. Zo is de informatie die wordt gegenereerd met behulp van de OV-chipkaart toegankelijk voor vele tientallen partijen, afkomstig uit zowel de publieke als private sector.

Een belangrijke vraag die samenhangt met toegankelijkheid is controle. Wie controleert en beslist over de toegang tot informatie? Controle en toegang kunnen niet los worden gezien van de technologische applicatie of drager waarop de informatie staat. Zo maakt internet het verspreiden en delen van informatie tussen een oneindig aantal personen mogelijk zonder dat hier een grote mate van centrale controle aan te pas komt. Voor de toegang tot de databanken van de Belastingdienst of de systemen van de AIVD daarentegen gelden strenge eisen. Fleck (1993) maakt een onderscheid tussen technologieën die zijn opgebouwd als een 'systeem' of als een 'configuratie'. Bij een systeem – een gesloten netwerk – is er een strenge afbakening van hoe de onderdelen op elkaar zijn afgestemd, waardoor overzicht en centrale controle mogelijk is. Deze systemen behouden hun vorm en betekenis in

verschillende contexten. Een 'configuratie' – een open netwerk – daarentegen is meer open en heeft verschillende vertakkingen en applicaties, waardoor centrale controle en overzicht problematischer zijn. Gebruikers hebben een veel grotere rol in het bepalen van de werking van een configuratie dan van een systeem. Het is niet zo dat er één duidelijke actor valt aan te wijzen die de informatiestromen in de maatschappij beheerst. Enerzijds is er door de massale toegang tot pc's en internet de overtuiging dat gebruikers zelf steeds meer controle krijgen over hun informatie (Gilder 1994; Dutton 1999; Frissen 2008; Leadbeater 2008), anderzijds wordt beargumenteerd dat ICT-innovaties een nieuwe elite van *cybercrats* of *numerati* creëren (Ronfeldt 1992; Baker 2008). Informatie blijkt in de praktijk van alledag in ieder geval niet altijd en niet voor iedereen beschikbaar, zo illustreert onder meer het initiatief van de overheid om gezamenlijk met internetproviders te werken aan een zwarte lijst met verboden internetpagina's. De pagina's op deze lijst worden geblokkeerd en zijn daarmee niet toegankelijk voor het publiek.[1]

Maar het gaat om meer dan uitsluitend toegang tot informatie en de controle op die toegang. De grote uitdaging anno 2011 is niet zozeer om meer gegevens te verzamelen – dat gaat als het ware 'vanzelf' – maar om, gegeven een bepaald (beleids)doel, uit de massa aan data de *relevante* informatie en uiteindelijk ook *kennis* te vergaren (Hildebrandt & Gutwirth 2008: 1). Naast toegankelijkheid en controle is een tweede betekenisvol kenmerk van de huidige informatie- en kennismaatschappij daarom de wijze waarop *informatie omgezet wordt in kennis.* Evenzeer geldt dat voor de keuze *welke data wel of juist niet worden omgezet in informatie.* Kortom, het gaat niet om informatie als zodanig en de hoeveelheid daarvan, maar om de informatie die relevant is en om de (nieuwe) kennis die uit de berg aan informatie valt te destilleren. Om de overvloed aan data het hoofd te bieden wordt de selectie van informatie daarom meer en meer geoptimaliseerd en daarbij ook steeds vaker geautomatiseerd. De meest bekende toepassing hiervan is de zoekmachine Google die, op basis van een algoritme, websites rangschikt aan de hand van de ingetypte zoektermen en de gebruiker vervolgens zo snel mogelijk naar de internetpagina met het 'gewenste' antwoord leidt. Het proces van zoeken naar opvallende patronen of correlaties in de data door middel van een algoritme wordt ook wel *data mining* genoemd (Custers 2004). Data mining levert correlaties op die duiden op een relatie tussen data, zonder per se ook een oorzaak voor of causaliteit van die relatie bloot te leggen (Hildebrandt 2008: 18). Een andere bekende data-miningapplicatie is de service die bijvoorbeeld online boekenverkopers als Bol.com en Amazon leveren. "Lezers die het WRR-rapport *Identificatie met Nederland* kochten, bestelden ook het WRR-rapport *Onzekere Veiligheid.*" Hierbij leidt data mining tot het vormen van profielen (een verzameling van correlerende data), wat ook wel *profiling* wordt genoemd (zie Canhoto & Backhouse 2008). De online aankopen van consumenten, het gedrag van jongeren, het bestedingspatroon van uitkeringsgerechtigden worden gecategoriseerd en gebruikt om voorspellingen over hun toekomstig gedrag te doen. Profilering vindt daarbij

plaats op twee assen: het gedrag van het individu in het verleden (bepaald koopgedrag, ziektepatroon, enz.) gekoppeld met het gedrag van de massa in het verleden. De correlaties staan voor de waarschijnlijkheid dat zaken die in het verleden op een bepaalde manier zijn gegaan, ook in de toekomst een soortgelijk verloop zullen kennen (Hildebrandt 2008: 18). De inzet van profielen beperkt zich niet tot de commerciële sector. Ook de overheid gebruikt de toepassing inmiddels op diverse beleidsterreinen (belastingen, sociale zekerheid, jeugdgezondheidszorg, toezicht en handhaving). Aan de hand van 'burgerprofielen' oftewel burgerbeelden is een meer persoonsgerichte benadering mogelijk, zijn doelgroepen meer centraal te stellen, valt burgers werk uit handen te nemen of hoeft de overheid hen niet langer 'lastig te vallen' (Van der Hof et al. 2009).

Box 2.2 Risicoprofielen

Een illustratief voorbeeld van een volledig geautomatiseerde risicoanalyse gebaseerd op risicoprofielen is te vinden in de nieuwe aanpak voor het toezicht op rechtspersonen (Tweede Kamer 2008-2009f). Het huidige systeem van preventief toezicht wordt vervangen door permanent geautomatiseerd toezicht via risicoanalyses. Daarbij wordt ook gebruikgemaakt van gegevens over individuele personen, zoals over kinderen en kleinkinderen van bestuurders. De risicoanalyse is gebaseerd op risicoprofielen en risico-indicatoren die periodiek door de minister van Justitie worden vastgesteld. Elk risicoprofiel bestaat uit een set van risico-indicatoren (die op een risico voor misbruik wijzen) of kenmerken die in onderlinge samenhang (kunnen) wijzen op een vorm van misbruik. De betrokkenheid van familieleden (kinderen en kleinkinderen) bij de rechtspersoon is een voorbeeld van een risico-indicator. De gegevens die in de analyse worden meegenomen zijn afkomstig van onder meer de Belastingdienst, het Kadaster, het Handelsregister, de GBA, de politie en uitvoeringsinstanties voor werknemersverzekeringen. Hoe meer risico-indicatoren er in het geding zijn, hoe hoger de risicoscore van de rechtspersoon is. Bij elke wijziging in de 'levensloop' van de rechtspersoon wordt de rechtspersoon via automatische analyse langs de risicoprofielen geleid. Het gaat volgens de memorie van toelichting bij het wetsvoorstel naar verwachting jaarlijks om enkele honderdduizenden mutaties in levensloopmomenten. Op basis van de risicoscore kan een hogere prioriteit aan het toezicht op de rechtspersoon worden toegekend. De risicomeldingen worden volledig geautomatiseerd verstrekt aan diverse bij AMvB (Algemene Maatregel van Bestuur) aan te wijzen handhavende instanties. Individuen hoeven niet op de hoogte te worden gesteld dat hun gegevens zijn gebruikt bij een risicomelding.

Profilering wint in de publieke sector met name aan populariteit vanuit de wens tot proactief handelen. Daarmee zet de overheid overigens soms ook stappen die verdergaan dan alleen burgers identificeren en typeren. De ambitie is om aan de hand van de gegenereerde kennis ook een voorschot op de toekomst te nemen. Met behulp van profileringstechnieken zijn plichten, rechten en noden van specifieke burgers niet alleen in een vroeg stadium in te schatten, maar kan ook tijdig gehandeld en (bij)gestuurd worden. Zo werkt de politie met het signalerings-

instrument Prokid voor kinderen jonger dan twaalf jaar (twaalfminners), die op de een of andere wijze in relatie staan tot een strafbaar feit (waaronder zij die uitsluitend getuige zijn van een misdrijf). De risicotaxatie van Prokid werkt met twee bronnen van gegevens. Ten eerste wordt gebruikgemaakt van gedragsindicatoren waarvan wordt vermoed of vaststaat dat die tot criminele activiteiten kunnen leiden. Ten tweede kijkt men naar de gegevens die bekend zijn over de medebewoners op het woonadres van de twaalfminner en beoordeelt of die aanleiding geven tot verhoogd risico op crimineel- en probleemgedrag van de jongere. Op basis van de combinatie van deze twee bronnen van gegevens – het kind zelf en zijn woonomgeving – wordt het ingedeeld in een van de risicocategorieën. Aldus kan vroegtijdig worden gesignaleerd of het risico bestaat dat een kind crimineel of probleemgedrag zal ontwikkelen (Keymolen & Prins 2011).

Box 2.3 Vals positieve en vals negatieve risico's op het vliegveld

Bij het werken met nieuwe technologie als biometrie, maar ook met risico's en risicoprofielen kunnen twee verschillende soorten fouten worden gemaakt, met heel verschillende gevolgen. Op het vliegveld worden passagiers straks gecontroleerd met behulp van een biometrisch paspoort. Via de vergelijking van de vingerafdruk van de passagier en de vingerafdruk die op het paspoort is opgeslagen wordt gecontroleerd of de houder en het paspoort bij elkaar horen.

Naast de gewenste uitkomst (de vingerafdruk van de houder en die op het paspoort zijn van één en dezelfde persoon) kan er ook een *vals negatieve uitslag* zijn (de vingerafdruk van de houder en die op het paspoort matchen bij de controle niet, terwijl ze wel van één en dezelfde persoon zijn) of een *vals positieve uitslag* (de vingerafdruk van de houder en die op het paspoort matchen bij de controle wel, terwijl ze in werkelijkheid niet van één en dezelfde persoon zijn). De eerste fout zorgt voor veel frustratie bij de reiziger, voor uitgebreide verdere controle van de identiteit van de reiziger en resulteert niet zelden in een gemist vliegtuig. De tweede fout zorgt ervoor dat mensen toegang tot Nederland krijgen die geen toegang hadden mogen krijgen. De ultieme vrees is daarbij dat het om illegalen, criminelen of zelfs terroristen gaat.

In de techniek die op vliegvelden wordt gebruikt, zoals biometrische toegangssystemen, geldt echter dat de foutmarges voor dit soort inschattingen eenvoudigweg 'ingesteld' kunnen worden. En dat gebeurt ook. Het herkennen van een vingerafdruk kan bijvoorbeeld op 99 procent zekerheid worden ingesteld, maar ook op 80 procent zekerheid. Het eerste heeft veel meer controle en lange rijen tot gevolg, maar maakt de kans op vals positieve uitkomsten (iemand krijgt toegang, terwijl hij niet bij zijn biometrisch paspoort hoort) bijna nihil. Het tweede komt de doorstroming op een vliegveld ten goede, maar vergroot de kans op onterechte toegang van personen die niet bij hun paspoort horen. Veiligheidsdiensten zullen meestal het eerste bepleiten, terwijl de commerciële en economische belangen – ook die van de staat! – naar het tweede neigen. Het een kan tegen het ander worden uitgeruild en vals positieve en vals negatieve fouten zijn dus tot op zekere hoogte communicerende vaten.

Het groeiende besef dat de uitdaging niet zozeer ligt in het puur verzamelen van grote hoeveelheden informatie, maar in het traceren van de *relevante* informatie en de nieuw te genereren kennis, zet behalve profilering nog een tweede aandachtspunt op de agenda: informatie over informatie (metadata). Juist omdat technologie het mogelijk maakt om steeds maar meer gegevens te verzamelen en aan elkaar te koppelen, is de vraag naar een (technologische) oplossing voor het vinden, duurzaam toegankelijk houden en daarmee dus structureren van die gegevens alleen maar groter geworden. Zogenaamde metadata (gegevens die iets zeggen over een bepaalde set van documenten of brok informatie) spelen bij zowel het duurzaam toegankelijk maken als het structureren van gegevens een belangrijke rol. Veel hedendaagse technologische applicaties zijn zo ontworpen dat ze automatisch data genereren over datgene wat ze doen of voortbrengen. Een faxapparaat zet automatisch een datum op de in- en uitgaande post, een digitale camera 'onthoudt' wanneer een foto is gemaakt, een camera met GPS slaat op waar de foto of film is gemaakt en sommige auto's 'onthouden' hoe hard op een bepaald tijdstip is gereden. Deze data over het betreffende object (fax, foto, film of auto) maakt het mogelijk om zaken gemakkelijker te ordenen en terug te vinden. Ook in de relatie overheid-burger groeit het belang van beschikbare metadata, omdat het van invloed is op de machtsposities van de betrokken actoren.

Een belangrijke ontwikkeling in het zoeken en vinden van relevante informatie is dat indexen en zoekfuncties in één interface worden geïntegreerd, waardoor alle informatieniveaus gezamenlijk worden weergegeven. Met andere woorden, het ouderwetse onderscheid tussen zoeken op bestandsniveau (kaartenbak) en in het bestand zelf (in het dossier – de inhoud) vervaagt (Mayer-Schönberger 2009: 77). Tegelijk zijn er ook ontwikkelingen om toegang met behulp van metadata te reguleren. Zo bestaat de mogelijkheid via de metadata van een bestand (boek, artikel, film, muziek, enz.) op te slaan wie toegang heeft tot de desbetreffende informatie en hoe ver die toegang reikt (bijv. alleen lezen of ook aanpassen). Inmiddels klinkt de roep om regulering van eigendom op en gebruik van metadata, vanuit het besef dat "metadata, concentrating the sea of data to make it comprehensible, also can act as a bottleneck on information access and is an instrument of market power" (Cukier 2010: 10).

2.3 DE ACTOREN CENTRAAL

De twee voorgaande paragrafen bepalen in grote lijnen de gekozen aanpak. De afbakening van het socio-technologisch systeem betekent dat de focus van de analyse ligt op het samenspel van actoren zoals burgers, instituties en applicaties. Het is dit samenspel dat uiteindelijk bepaalt hoe de dynamiek tussen informatie en technologie eruit komt te zien. Om deze actoren in beeld te krijgen is ten behoeve van dit rapport empirisch onderzoek uitgevoerd naar specifieke applicaties en literatuuronderzoek in de vorm van domeinstudies, gericht op het bredere

(beleids)terrein. Het empirisch onderzoek, tezamen met de (wetenschappelijke) literatuur en de gesprekken en interviews gehouden met spelers in het veld van 'ICT en overheid', vormen de bouwstenen voor de visie die in dit rapport wordt ontwikkeld. Het gaat daarbij om de algemene patronen en inzichten die kunnen worden afgeleid uit de analyses van de verschillende applicaties. De voornaamste actoren die worden gevolgd zijn de burger, de overheid en de applicatie. Dit zijn natuurlijk niet de enige partijen die invloed uitoefenen op de ontwikkeling, implementatie en doorwerking van ICT. Ook het bedrijfsleven en belangengroepen spelen dikwijls een belangrijke rol. Zij komen in dit onderzoek echter pas in beeld wanneer ze raken aan de interacties tussen de drie leidende actoren: burger, overheid en applicatie. Deze drie centrale actoren worden hieronder toegelicht.

2.3.1 SCHETS VAN DE ACTOREN

'De' burger en 'de' overheid zijn nuttige abstracties: constructen die houvast geven en die het mogelijk maken te redeneren over burgers of overheden in verhouding tot elkaar en andere actoren. In werkelijkheid valt de burger uiteen in vele verschillende burgers en de overheid in vele verschillende overheden, die bovendien tegengestelde belangen en voorkeuren kunnen hebben. Er bestaat uiteraard wel zoiets als 'de' overheid als het gaat om de juridische en politieke relatie met de burger. Om 'applicaties' als actor te kunnen beschouwen is een andere vorm van abstractie nodig, aangezien een applicatie moeilijk een eigen wil toegeschreven kan worden. Maar technologie kan wel het doen en laten van mensen beïnvloeden als gevolg van het ontwerp en de functie die een applicatie heeft gekregen.

2.3.2 'APPLICATIES'

In het rijtje van actoren is technologie, en meer specifiek de technologische applicatie, dus de vreemde eend in de bijt. Actoren roepen de associatie op van handelen en handelen gebeurt vaak vanuit een bepaalde overtuiging of intentie. Dat technologische applicaties hier als actoren worden gezien betekent niet dat zij ook intentionaliteit of een eigen wil toegedicht krijgen. Het belangrijkste criterium om een applicatie als actor te zien is het feit dat de aanwezigheid daarvan 'iets doet' in interacties. Een actor is iets of iemand die een *verschil* maakt in een relatie (Latour 2005). Met andere woorden, technologische applicaties, zoals het EPD en het biometrisch paspoort, geven de relatie tussen burgers en overheid op een bepaalde manier vorm. Hun aan- of afwezigheid maakt uit. Om te kunnen begrijpen waarom acties plaatsvinden en hoe burgers en overheden interacteren, moeten ook de objecten die deze acties mogelijk maken in de analyse betrokken worden. Dat technologische applicaties invloed uitoefenen op het handelen van burgers en overheden kwam al eerder in dit hoofdstuk naar voren. Technologische applicaties die ingebed zijn geraakt in de maatschappij krijgen een eigen gewicht, waardoor bijsturing moeilijk wordt en bepaald menselijk handelen beknot of juist gestimu-

leerd wordt. Technologische applicaties hebben bovendien niet alleen bedoelde maar ook onbedoelde en onverwachte gevolgen die de interacties en het handelingsperspectief van actoren beïnvloeden. Zo was sms bij de introductie van de mobiele telefoon niet meer dan een grappig extraatje. Het gebruik van deze dienst nam onverwachts echter zo'n grote vlucht dat het niet alleen een belangrijke manier van communiceren is geworden (zeker onder jongeren), maar ook op andere niveaus in de maatschappij invloed heeft, bijvoorbeeld op de ontwikkeling van de taal.

Dat technologische applicaties ook in de dagelijkse praktijk een actorschap bezitten blijkt uit de manier waarop mensen omgaan met technologie zoals computers, televisies en telefoons. Uit psychologisch onderzoek blijkt dat mensen dezelfde sociale regels toepassen in interacties met computer en televisie die ze ook gebruiken bij interpersoonlijke interacties (Reeves & Nass 1996). Er wordt ook wel gesproken van het CASA-paradigma: Computers Are Social Actors (Nass et al. 1994; Nass et al. 1995). Hierbij is het wederom niet noodzakelijk allerlei intenties of autonomie toe te dichten aan computers. Computers bezitten geen emoties, maar ze kunnen die wel teweegbrengen bij gebruikers, waardoor deze op hun beurt gaan geloven dat er wel degelijk emoties in het spel zijn bij interacties met technologische applicaties (Nusselder 2007: 9). Het feit dat mensen computers behandelen als sociale actoren maakt dat ontwerpers hun technologische applicaties soms zo proberen te ontwikkelen dat ze nog meer aan deze verwachtingen voldoen, bijvoorbeeld door spraaktechnologie en feedbackinformatie aan applicaties toe te voegen (Klein 2003). Tenslotte worden technologische applicaties wanneer ze moeten functioneren als expertsystemen bewust zo ontwikkeld dat ze in de relatie met de gebruiker het handelingsvermogen overnemen. Illustratief zijn de automatische piloot die bepaalde handelingen overneemt van de piloot en een remsysteem in een auto dat automatisch in werking treedt wanneer een voorligger abrupt vertraagt. Ook in de relatie overheid-burger kan ICT structurerend en sturend werken. Bovens en Zouridis (2002) signaleren een ontwikkeling waarin de *street level bureaucrat* verandert in een *screen level bureaucrat*. Professionals zien hun discretionaire ruimte afnemen als gevolg van de keuzes en beslisbomen die geprogrammeerd zijn in de gebruikte software (zie ook Meijer 2009; Lyon 2009). De applicatie bepaalt welke informatie relevant en juist is en de leiding of bestuurlijk verantwoordelijken bepalen welke applicatie gebruikt wordt. In deze infocratie (Zuurmond 1994) worden professionals in hun handelen, maar zeker ook in hun waarnemingen meer en meer gestuurd door de applicaties waarmee ze werken. Sommige lokale verwijsindexen voor het signaleren van risicojongeren zijn technisch zo ingericht dat een jongere die "bij de intake op basis van bepaalde criteria wordt aangemerkt als een jongere met een hulpvraag 'automatisch' wordt opgenomen" (Holla 2008: 13). Kortom, het is in dit geval niet langer aan de arts, jeugdhulpverlener of andere professional om te bepalen of al dan niet een risicosignaal in het systeem wordt afgegeven.

Ook is voor gebruikers de output van een technologische applicatie lang niet altijd te controleren op accuratesse. De cijfers, statistieken en waarschuwingen rollen kant en klaar uit de computer en de gebruiker kan niet anders dan varen op de informatie die door het systeem wordt aangeleverd. Van den Hoven (1998) typeert deze technologische applicaties als *artificial authorities*. Gebruikers zijn in grote mate eenzijdig afhankelijk van de, door deze applicaties voortgebrachte, informatie. Overigens zijn gebruikers en professionals natuurlijk geen volledig weerloze slachtoffers van ICT. Zij zoeken binnen of buiten het systeem naar werkbare oplossingen waarbij de menselijke controle gegarandeerd blijft (Van den Akker & Kuiper 2008).

2.3.3 'BURGERS'

Dat 'de' burger uiteenvalt in vele (groepen) burgers is geen verrassing. Gerelateerd aan de thematiek van dit rapport kan dat worden ingekaderd aan de hand van twee assen: die van de relatie burger-informatietechnologie en die van de relatie overheid-burger.

In hun relatie tot informatietechnologie kunnen burgers sterk verschillen in termen van kennis, vaardigheden, houding, belangen en wensen. Hoewel ICT als maatschappelijk fenomeen nauwelijks uit het dagelijkse leven weg te denken is, bewegen Nederlandse burgers zich met verschillende snelheden en met meer of minder enthousiasme door het digitale leven. Naast de mensen die ICT enthousiast omarmen staan mensen die bewust niet mee willen doen (Wyatt 2003; Van Dijk 2007; Van den Berg 2009) of achterblijven bij de snelle ontwikkelingen, zoals vooral ouderen, laagopgeleiden, lage inkomensgroepen en sommige etnische minderheden (CBS 2009a; Van Dijk 2007). Wat wel en niet aanslaat is bovendien vaak een onvoorspelbaar proces dat wel de domesticatie van technologie wordt genoemd (Frissen 2004). Silverstone en Hirsch (1992) omschrijven domesticatie als "a taming of the wild and a cultivation of the tame" (gecit. in Oudshoorn en Pinch 2003: 14). In het proces van domesticatie verandert zowel de gebruiker als de technologie. Als het gaat om de rollen en wensen die verschillende burgers hebben kan ICT ook een belangrijke rol spelen. De politieke activist, de patiënt met een zeldzame ziekte, de expat die in contact wil blijven of simpelweg de burger die een sociaal netwerk wil onderhouden, allemaal hebben ze een digitaal leven dat dikwijls groeiende is.

Steeds vaker treden burgers en overheden ook in een digitale omgeving met elkaar in contact. Als klant van de overheid, als belastingbetaler, als patiënt, als burger die veilig over straat wil en als stemmer. Soms zijn posities en belangen van deze rollen tegenstrijdig: een patiënt wil goede gezondheidszorg en is vanuit die positie wellicht een voorstander van het EPD. Tegelijkertijd is een (wellicht dezelfde) patiënt lid van een 'lotgenoten' website, die actief druk uitoefent op het beleid.

Bovendien kan een (wellicht wederom dezelfde) patiënt uit overwegingen van privacy zich als (politiek) burger grote zorgen maken over het EPD. Zeker als het gaat om het metaniveau van de rol die technologie in het dagelijkse leven en in het overheidsbeleid moet spelen, geldt dat de belangen van burgers ver uiteen kunnen liggen. Sommige burgers liggen niet wakker van de informatie die overheden (over hen) verzamelen, terwijl anderen daar fanatiek voor of tegen zijn. Andere burgers staan er eenvoudigweg niet bij stil. Recenter onderzoek laat zien dat burgers meer en meer variëteit aanbrengen in hun opvattingen over het gebruik van informatie. Het onderzoek dat de WRR uitvoerde in samenwerking met ECP-EPN en Centerdata laat zien dat de respondenten heel specifieke ideeën hebben over wie voor welk doel welke digitale gegevens mag gebruiken (Attema & De Nood 2010: 2). Bovendien willen burgers iets retour voor hun steun aan de initiatieven: ruimere mogelijkheden tot inzage en correctie. Zo vindt meer dan 80 procent dat voor jeugdzorg (EKD) en gezondheidszorg (EPD) professionals de digitale gegevens moeten kunnen inzien. Maar tegelijkertijd vindt 70 procent dat betrokken ouders of de patiënt zelf de digitale gegevens in moet kunnen zien, moet kunnen corrigeren en moet kunnen weten aan wie de gegevens zijn doorverstrekt (Attema & De Nood 2010: 2).

In termen van informatie geldt dat de informatiesamenleving burgers zowel meer als minder ruimte geeft om zich in verschillende hoedanigheden te presenteren. Via *social network sites* (Facebook, Hyves) en professionele netwerksites (LinkedIn) kan iedereen dat beeld van zichzelf neerzetten dat hij of zij aan de wereld, of een kleinere digitale kring, wil tonen. Tegelijkertijd geldt dat informatie die op het internet terechtkomt zich in een razend tempo onttrekt aan het beheer en controle van de persoon die het erop geplaatst heeft (Mayer-Schönberger 2009). Niet alleen kan informatie in een heel andere context opduiken dan die waarvoor ze bedoeld was – met alle gevolgen van dien –, maar door het netwerkkarakter van internet verspreidt informatie zich snel. Hoe burgers waargenomen worden en welke informatie over hen beschikbaar is hangt daarom maar ten dele van het eigen handelen van burgers af. Vervolgens hebben zowel bedrijven als overheden grote belangstelling voor de burger in zijn vele rollen en gedragingen, zowel op individueel niveau als op geaggregeerd niveau (Baker 2008; Mayer-Schönberger 2009). Mayer-Schönberger (2009: 104) meldt dat er Amerikaanse bedrijven zijn die dossiers aanbieden met meer dan 1.000 *individual data points per person* voor miljoenen Amerikanen. 'Burgers' en 'klanten' worden bovendien steeds meer benaderd op basis van hun digitale representaties die in verschillende databanken zijn opgeslagen (Baker 2008). Door middel van software wordt gezocht naar patronen in de massa van de opgeslagen data: het eerdergenoemde profiling en data mining zijn daarvan de meest bekende voorbeelden. Dit leidt er volgens Clarke (1988) toe dat *surveillance* steeds meer *dataveillance* wordt: niet de directe waarneming van een persoon bepaalt de aard van het toezicht, maar het verzamelen en bewerken van reeds opgeslagen informatie over personen en gedrag. Deze

worden door Haggerty en Ericson (2000: 613) wel *data-doubles* genoemd: elektronische profielen, vaak samengesteld uit een combinatie van verschillende datafragmenten over een bepaalde persoon, die na verloop van tijd zelfstandig gebruikt worden en een eigen realiteit gaan vormen. Clarke (1994) spreekt in dit verband ook wel over *the digital persona* en Solove (2004) van *digital persons*. Deze manier van bewerken en benaderen heeft belangrijke gevolgen voor burgers: hun digitale identiteit bestaat steeds meer uit informatie die is gedecontextualiseerd en die bovendien nauwelijks nog uit het digitale geheugen van 'het net' en de dataverzamelaars die daarvan gebruikmaken te verwijderen is (Mayer-Schönberger 2009; Prins 2009; Buruma 2011).

Box 2.4 Burgers hebben geen bezwaar tegen 'opspoorbaar' op het internet zijn

De politie is niet alleen aanwezig op straat, maar ook op het internet. Daar speurt ze op *social network sites* als Hyves, Facebook en Marktplaats naar sporen die gebruikt kunnen worden bij opsporingsonderzoek. Ook de Belastingdienst zoekt het internet af naar relevante gegevens over het wel en wee van belastingplichtigen. De burgers die deelnamen aan het onderzoek van ECP-EPN en de WRR geven deze instanties veel ruimte om de 'openbare' gegevens (gegevens die niet met een wachtwoord of op een andere manier zijn geblokkeerd) op internet te gebruiken. 80 procent van respondenten vindt dat de politie op internet naar gegevens mag speuren. Bijna 60 procent vindt dat de Belastingdienst mag zoeken naar openbare internetgegevens. Van de gegevens die zijn geblokkeerd en zijn beveiligd vindt 50 procent dat de politie die mag bekijken voor opsporingsdoeleinden. Bijna 40 procent van de respondenten vindt dat de Belastingdienst internetgegevens die zijn geblokkeerd of beveiligd mag raadplegen (Attema & De Nood 2010).

2.3.4 'OVERHEDEN'

Ook de overheid valt in vele overheden uit elkaar. Hoewel 'de' Nederlandse overheid in beginsel één entiteit is (mooi samengevat in de grondwettelijke idee dat Nederland een decentrale eenheidsstaat is) geldt in de dagelijkse praktijk dat de overheid vele rollen en gezichten aanneemt. De overheid onderscheidt zich zowel via verschillende posities – politiek, beleid, management en uitvoering – als via verschillende instanties – de Belastingdienst, de politie, enzovoorts. Niet in de laatste plaats onderscheidt de overheid zich ten opzichte van de burger. Deels is dat niet nieuw; wie als burger in aanraking komt met de politie ziet een andere overheid dan wanneer hij of zij te maken krijgt met de Belastingdienst of het gemeentehuis. Toch zijn deze allemaal representanten van dé overheid waarmee burgers te maken hebben en waardoor burgerschap – in zijn politieke betekenis – inhoud heeft. Ook voor de overheid geldt dat deze op twee assen kan worden ingekaderd: die van de relatie overheid-informatietechnologie en die van de as overheid-burger.

Informatietechnologie verandert ook de overheid – of beter: overheden – zelf. Informatie, communicatie en dienstverlening van overheden worden in hoog tempo gedigitaliseerd, waarmee niet alleen het gezicht van de overheid verandert, maar ook veel van de (interne) werkprocessen. Net als bij burgers geldt daarbij dat de 'ICT-revolutie' verschillende overheden op verschillende manieren en snelheden heeft geraakt en raakt. ICT heeft de interne (informatie)huishouding en werkprocessen van de overheid sterk veranderd (Dunleavy et al. 2006), maar doet meer dan alleen de weberiaanse bureaucratie versnellen en efficiënter maken. Het transformeert ook de manier waarop overheden interacteren met andere actoren, zowel binnen als buiten de overheid. Interactie met burgers verandert als een loket een internetpagina wordt of een paspoort de scan van een vingerafdruk. Iets wat in eerste instantie een moderne versie van hetzelfde lijkt – de eerste auto's leken ook gemotoriseerde koetsen – blijkt zich na verloop van tijd door te ontwikkelen. Het karakter van de overheid was in de laatste decennia al aan het evolueren op een manier die sterk aansluit bij de mogelijkheden die ICT biedt. De institutionele differentiatie, de europeanisering, de internationalisering en de liberaliserings- en verzelfstandigingsoperaties van de jaren negentig hebben van Nederland volgens Dijstelbloem en Holtslag (2010: 15), met verwijzing naar Majone, een *regulatory state* gemaakt: naast de traditionele decentrale lagen heeft 'de' overheid zich over een veelheid aan overheids- en semi-overheidsinstellingen verspreid. Daarmee is de overheid steeds meer een netwerkoverheid geworden, een ontwikkeling die goed past bij, en verweven is met het netwerkpotentieel van ICT.

Hoe de overheid ICT benut en op welke wijze een digitaal overheidsnetwerk functioneert, hangt voor een groot deel af van de aard van de relatie tussen burger en overheid. Bezien vanuit de overheid kan die relatie van burgers en overheid worden getypeerd in drie categorieën: *service, care & control* (dienstverlening, zorg en controle). Dit zijn uiteraard brede categorieën[2] die in analytische zin wel van elkaar te onderscheiden zijn, maar in praktische zin sterk door elkaar lopen. Daar zijn verschillende redenen voor aan te wijzen. De ontwikkeling van de eOverheid was, zoals hoofdstuk 1 introducerend schetste, in eerste instantie sterk gegrond in het verbeteren en efficiënter maken van de dienstverlening van de overheid. Maar meer recent is de inzet van ICT ook populair in de zorg (bijv. welzijn, gezondheidszorg of jeugdzorg) en bij controle en handhaving (bijv. politie, immigratie en terrorismebestrijding). Daarbij zet de overheid overigens mede in op de emancipatoire mogelijkheden die ICT voor dienstverlening, zorg en controle in petto heeft: de digitale dienstverlening moet *citizen-centric* worden ingericht (Burger Service Kaart, Burgerservicenummer), ICT dient patiënten te emanciperen en hen langer zelfstandig te laten functioneren (Keizer 2011) en de politie roept burgers op met hun mobiele telefoon een bijdrage te leveren aan controle en handhaving.

Box 2.5 Begripsverwarring: keten of netwerk

Waar de wetenschap veelal spreekt over netwerken, hanteert de Nederlandse overheid in haar officiële stukken juist de term 'ketens' en een ketenbenadering. Dat doet ze ook op momenten dat – kijkend naar de applicatie – de term netwerk op z'n plaats is.

In een ketenbenadering werken organisaties en actoren samen om een probleem op te lossen of een doel te bereiken. De verbinding in de keten komt niet voort uit een overkoepelend gezag dat hierop stuurt, maar de behoefte van verschillende organisaties aan elkaars product of informatie (Grijpink 2006a). De keten is een lineair proces waarin verschillende organisaties buiten hun eigen organisatiegrenzen werken aan een gemeenschappelijk resultaat (Borst 2009). De volgorde waarin onderdelen en actoren hun plaats in de keten innemen, wordt bepaald door het probleem dat opgelost moet worden, dan wel de dienst of product die geleverd moeten worden. Voor het goed functioneren van de keten zijn alle onderdelen en actoren noodzakelijk.

Naast de opkomst van ketens, zijn (zowel publieke als private) organisaties steeds vaker verbonden met andere organisaties in een netwerk. De term 'netwerk' verwijst naar een relatief open verband waarbij verschillende onderdelen (knooppunten) in relatie staan tot andere onderdelen via veelvoudige, doorkruisende en vaak redundante verbindingen. Via deze verbindingen beweegt informatie zich van het ene onderdeel naar het andere (Barney 2004). In tegenstelling tot bij ketens zijn er in een netwerk dus alternatieve mogelijkheden om uitwisseling tot stand te brengen. De stromen bewegen zich in verschillende richtingen, wederkerig of in één richting, en mogelijk via meerdere vertakkingen. Verbindingen kunnen bovendien sterk of zwak, enkelvoudig of meervoudig zijn. Vanwege het dynamische, flexibele en adaptieve karakter is een netwerk moeilijk te coördineren en sturen (Castells 1996). Alhoewel binnen de overheid in principe iedere informatiestroom is gereguleerd, informatie daarmee niet 'vrij stroomt' maar volgens wettelijke gedetermineerde routes en aldus gesproken zou kunnen worden van ketens, is de dagelijkse realiteit soms een andere en is in feite sprake van een netwerk. Door te spreken in termen van ketens waar het in werkelijkheid netwerken betreft, wordt deze complexiteit door de overheid onvoldoende onderkend.

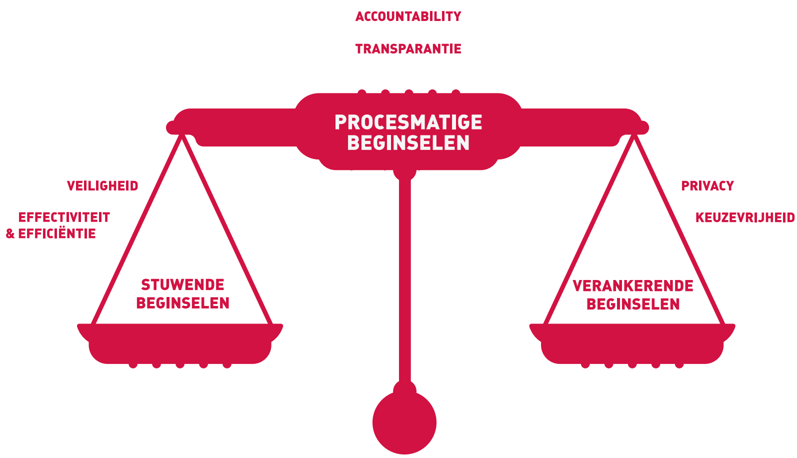
De analyse in deel II laat zien dat innovatie in digitale dienstverlening tegelijkertijd ook nieuwe mogelijkheden biedt om burgers te observeren en te controleren. Kortom: zonder bureaucratie geen Big Brother, maar ook geen verzorgingsstaat. Daarbij illustreren diverse initiatieven dat de grens tussen service, care en control steeds diffuser wordt. Soortgelijke ontwikkelingen worden ook in andere landen waargenomen (Lips, Taylor & Organ 2009). Als archiefkasten in hoog tempo worden omgezet in digitale databanken die koppelbaar en snel en op afstand doorzoekbaar zijn, nemen de mogelijkheden voor nieuwe vormen van samenwerking ook sterk toe. Dat geldt voor digitale dienstverlening, voor digitale zorg en voor digitale controle. De *surveillance* van de burger door de overheid bevindt zich volgens Lyon (2007: 3) altijd ergens op het continuüm tussen care en control.

Verschillende auteurs wijzen erop dat bureaucratische registratie en documentatie zowel instrumenten van controle als instrumenten van verdelende rechtvaardigheid kunnen zijn (zie bijv. Lyon 1994; Marx 2001; Gilliom 2001). Maar ook om andere redenen zijn de grenzen tussen controle, dienstverlening en zorg lang niet altijd eenvoudig te trekken. Waar Foucault (1977) het had over een disciplinerende samenleving, waarin disciplinerende instituties als de gevangenis en de school centraal staan, spreken filosofische 'opvolgers' als Deleuze (2002) over een controlesamenleving, waarin controle een permanent proces is geworden dat zich heeft losgemaakt van fysieke locaties en daarmee ook van instituties. Juist onder invloed van deze ontwikkeling kunnen de grenzen tussen de verschillende hoedanigheden waarin de overheid zich tot burgers verhoudt (dienstverlenende, controlerende, zorgende overheid) in de dagelijkse praktijk gaan schuiven, waarmee de beleidscategorieën van service, care en control in elkaar over gaan lopen.

2.4 EEN ANALYTISCH DRIELUIK VAN BEGINSELEN

In de discussies rondom het ontwikkelingstraject van applicaties, of het nu gaat om het Elektronisch Patiëntendossier, het biometrisch paspoort of de OV-chipkaart, worden door actoren allerhande beoordelingsmaatstaven – zoals veiligheid, transparantie en keuzevrijheid – in de discussie ingebracht. Deze maatstaven worden ingebracht ter ondersteuning van een voorstel voor digitalisering, om de werking en het bereik ervan te beperken of te verruimen of om goede procedures voor het dagelijks gebruik van een applicatie te ondersteunen. Zulke maatstaven worden in dit rapport als beginselen aangeduid en geanalyseerd. Het zijn de begrippen aan de hand waarvan ICT-ontwikkelingen de maat genomen wordt, zowel door actoren in het veld als in deze analyse. Gedurende het hele proces maken actoren zich hard voor tal van beginselen. De uiteindelijke vorm die een applicatie krijgt – niet alleen de technologie zelf, maar ook haar sociale (bestuurlijke, juridische) inbedding en uitwerking – is een uitkomst van de strijd tussen de vaak tegenstrijdige ideeën en normatieve oriëntaties die zo in het spel worden gebracht. De empirische analyse in dit rapport zou in details en tegenstrijdigheden vastlopen wanneer deze beginselen allemaal een voor een onder de loep genomen zouden worden. Dit rapport werkt daarom met een *driedeling* van beginselen, die voor de analyse van groter belang is dan de individuele beginselen. Deze driedeling houdt een onderscheid in tussen stuwende, verankerende en procesmatige beginselen. De driedeling brengt helderheid in een vaak complex geheel van argumentaties over maatstaven door de meest relevante beginselen onder te brengen in drie betekenisclusters en die leidend te maken voor de analyse. Want wat de empirie in ieder geval glashelder aantoont, is dat een goede omgang met ICT in de relatie overheid-burger vraagt om afwegingen. Uiteindelijk kan immers niet volledig aan alle beginselen – hoe belangrijk ze ieder voor zich ook zijn – tegelijkertijd recht worden gedaan.

Figuur 2.1 Schematische voorstelling van de driedeling



Stuwende beginselen zijn beginselen die verbonden zijn met de *drive* van de overheid om ICT in tal van domeinen in te zetten. De stuwende beginselen staan in het teken van verbetering en kwaliteitswinst. In dit rapport worden twee, in het debat veelvoorkomende stuwende beginselen verder uitgewerkt: *veiligheid* en het ogenschijnlijk verstrengelde koppel *effectiviteit en efficiëntie*. De verankerende beginselen staan voor het waarborgen van vrijheden, het in kaart brengen van 'stille verliezen' bij voortgaande digitalisering en voor het vrijwaren van de autonomie van het individu. De verankerende beginselen vormen een tegenwicht voor de stuwende beginselen. Ze remmen de kracht van de stuwende beginselen af. *Privacy* en *keuzevrijheid* worden in dit rapport uitgelicht als twee belangrijke verankerende beginselen. Om tot een uitgebalanceerde applicatie of beslissing over de inzet van ICT te komen, moeten beginselen ten slotte tegen elkaar afgewogen worden. De procesmatige beginselen staan voor de procedurele omlijsting die het mogelijk maakt dat de stuwende en verankerende beginselen op een zorgvuldige manier gewogen worden. Deze afwegingsprocessen moeten vooral toetsbaar en inzichtelijk zijn. Van de procesmatige beginselen worden in dit rapport *transparantie* en *accountability* verder uitgewerkt.

Belangrijk is dat deze zes beginselen niet meer dan een operationalisering vormen van de categorieën van de driedeling. De zes beginselen die worden uitgewerkt spelen een prominente rol in de dynamiek rondom de inzet van ICT door de overheid, maar geven geen uitputtend beeld. Wel laten de beginselen die worden uitgewerkt de afwegingen tussen de stuwende, verankerende en procesmatige beginselen heel concreet 'zien', waardoor de analyse minder abstract wordt. Er spelen uiteraard nog wel meer normatieve noties een rol in het denken over ICT en overheid. Te denken valt aan toegankelijkheid, rechtmatigheid, rechtszekerheid, handelingsvrijheid of gelijkheid. De individuele beginselen kunnen noch limita-

tief worden opgesomd noch definitief worden gekenschetst, alleen al omdat de informatiesamenleving zich voortdurend blijft ontwikkelen.

Met de keuze voor een driedeling komt de nadruk te liggen op de *afweging* die (onder meer) de regering en het parlement moeten maken tussen verschillende, ongelijksoortige normatieve beginselen wanneer nieuwe technologieën worden geïntroduceerd. Telkens opnieuw moeten immers uiteenlopende en vaak tegenstrijdige beginselen als privacy, transparantie en veiligheid tegen elkaar worden afgewogen en met elkaar in balans worden gebracht. Deze afweging behelst dan ook geen toetsing aan de hand van individuele criteria. Een analyse bijvoorbeeld puur en alleen vanuit de stuwende beginselen, waarin alles in het teken staat van de vraag wat ICT al dan niet oplevert, veronachtzaamt immers al snel de 'zachtere waarden' (Nussbaum 2000) die in het geding kunnen zijn dan wel de procesmatige, democratische kwaliteit van de ontwikkelingen (Shrader-Frechette 1992: 131). De focus in dit rapport ligt veel sterker op de normatieve aard en de richting die de beginselen in het debat over ICT inbrengen dan op de individuele beginselen zelf. Met andere woorden, het gaat er in de analyse om wat de beginselen in de ontwikkelingen en debatten *doen*, niet zozeer om wat ze begripsmatig en inhoudelijk zijn. Een analyse van deze praktische invulling van de beginselen komt uitvoerig aan bod in deel II, bezien vanuit tal van beleidscontexten. Het wegen van ongelijksoortige beginselen vergt dan ook een andere aanpak dan bijvoorbeeld wordt gehanteerd door een orgaan als de Algemene Rekenkamer, die ICT-projecten met name langs de meetlatten van doelmatigheid en rechtmatigheid legt of de Nationale Ombudsman, die bij de toetsing van overheidsoptreden diverse behoorlijkheidsvereisten hanteert. De aanpak in dit rapport verschilt ook van de, vanuit de wetenschap ontwikkelde, normatieve criteria voor de inzet van ICT, zoals de door Franken geformuleerde beginselen van behoorlijk IT-gebruik (Franken 1993) en de door Bovens ontwikkelde informatierechten (Bovens 2003). Het wegen van ongelijksoortige beginselen vereist een ander soort exercitie dan het voldoen aan een relatief nauw omschreven lijst van criteria.

Hierna worden de stuwende, verankerende en procesmatige beginselen van de driedeling afzonderlijk besproken. In de eerste plaats wordt het karakter en de functie van elk van de drie categorieën uiteengezet. Ten tweede worden de concrete beginselen die onder elk van de drie categorieën vallen kort uiteengezet, om ten slotte, vooruitlopend op de empirische analyse in deel II, iets te kunnen zeggen over de confrontatie van en afweging tussen de stuwende, verankerende en procesmatige beginselen.

2.4.1 STUWENDE BEGINSELEN

De elektronische overheid wordt door een onmiskenbare dynamiek gekenmerkt. ICT stuwt de ambities van de overheid door nieuwe mogelijkheden voor beleid te

scheppen. Tegelijkertijd sluiten bepaalde ambities van de overheid – het verbeteren van de dienstverlening en het vergroten van de veiligheid – naadloos aan bij de nieuwe mogelijkheden die ICT biedt. Dat is bovendien geen exclusief Nederlands gegeven. In vele westerse landen leeft de ambitie om de eOverheid uit te laten groeien tot een klantgerichte, proactieve en efficiënte overheid die geen elektronisch middel onbenut laat om veiligheid en dienstverlening te optimaliseren. Hierin ondervindt zij weinig weerstand. Wie kan er tegen kwaliteitswinst en een daadkrachtige overheid zijn? In praktisch opzicht hebben stuwende beginselen weinig steun in de rug nodig om voor het voetlicht te treden.

Technologische vooruitgang in onder meer het veiligheidsdomein en de belofte van meer effectiviteit en efficiëntie door de inzet van nieuwe ICT-systemen eisen dat de overheid de vruchten van deze innovaties plukt. De aandrang om technologie in te zetten is groot, en niet ten onrechte. In de politiek-bestuurlijke afweging vertegenwoordigt de voorwaartse dynamiek van ICT een bijna vanzelfsprekende motivatie. Dankzij ICT ligt succes binnen handbereik en het gebruik ervan lijkt niet of nauwelijks nader te hoeven verantwoord. De belofte voor de toekomst en het eerdergenoemde technovertrouwen werken dit in de hand. Het ogenschijnlijke gemak waarmee technologische oplossingen worden aanvaard maakt echter ook dat de stuwende beginselen in het debat als vanzelfsprekend worden gezien, en daardoor eigenlijk nauwelijks zijn uitgekristalliseerd. Omdat er ogenschijnlijk geen tegenstanders zijn van meer effectiviteit en efficiëntie of van meer veiligheid, worden deze beginselen slechts weinig bevraagd. Door hun dominantiepositie in het maatschappelijke en beleidsmatige debat overschaduwen ze dan ook dikwijls andere belangen. In het krachtenveld van de dagelijkse praktijk hoeft voor de positie van de stuwende beginselen dus niet gevreesd te worden. Het gevaar schuilt eerder in de moeilijkheid een geloofwaardige, brede normatieve weging uit te voeren waar naast stuwende ook andere beginselen deel van uitmaken.

Effectiviteit en efficiëntie

Dat stuwende beginselen vaak geen onderwerp van een normatieve analyse zijn, maar in de praktijk weinig aandacht te kort komen, laat de inzet van de begrippen effectiviteit en efficiëntie in discussies over applicaties duidelijk zien. Effectiviteit is te omschrijven als het voldoen aan tevoren vastgestelde doelen. Efficiëntie wordt veelal gedefinieerd als het bereiken van een bepaald doel met zo min mogelijk middelen. Een verhoging van efficiëntie behelst dat 'hetzelfde' (het vooropgezette doel) met minder investeringen – in tijd, moeite en/of geld – kan worden gedaan. Hoewel effectiviteit en efficiëntie dus voor twee verschillende zaken staan, worden ze, met name wanneer het de dienstverlening aan de burger betreft, toch vaak in één adem genoemd. De potentie van ICT om beide doelen te dienen onttrekt eventuele tegenstellingen – efficiënt beleid kan heel ineffectief zijn – aan het oog.

Het tekort dat ontstaat wanneer men effectiviteit en efficiëntie vooral retorisch omarmt, door ze als een vanzelfsprekend en vaststaand kenmerk van ICT-initiatieven te beschouwen, toont zich met name bij de evaluatie van die initiatieven. Omdat men niet helder omschrijft wat precies onder effectiviteit en efficiëntie moet worden verstaan en hoe deze dienen te worden gemeten, is het moeilijk vast te stellen of doelstellingen zijn bereikt. Evaluatie is een wezenlijk onderdeel van de lerende (hoogtechnologische) overheid, of zou dat in elk geval moeten zijn. In het beleidsdiscours worden effectiviteit en efficiëntie echter vaak geponeerd of verondersteld, als zou de enkele bewering dat iets effectief en efficiënt is een *knock-out*-argument behelzen. Echte verantwoording van de claims die in het kader van de elektronische overheid worden gemaakt, ontbreekt vaak, zoals nader in deel II zal worden besproken.

Effectiviteit en efficiëntie waren altijd al van groot belang voor de overheid, maar spelen onder invloed van de mogelijkheden van ICT een steeds grotere rol. Dit heeft te maken met het prominenter worden van prestatie-indicatoren, doelmatig handelen en vormen van doelregulering in zowel private als publieke contexten. Zo staat in de politieke discussie over het EPD het aantal patiënten van wie het leven kan worden gered centraal (Pluut 2010) en wordt het succes van de Verwijsindex Risicojongeren afgemeten aan de hand van het aantal risicomeldingen (Keymolen & Prins 2011). Ambities als klantgerichtheid, resultaatgerichtheid en bedrijfsmatig werken maken de kern uit van de New Public Management-filosofie, waarin gepropageerd wordt dat de overheid zich in belangrijke mate naar bedrijfsmatig model moet hervormen. Alhoewel dat denken inmiddels wordt gerelativeerd, staan effectiviteit en efficiëntie nog steeds prominent op de agenda van het publieke management (De Groot 2010).

Wie kijkt naar de beleidsdocumenten en rapporten die de afgelopen jaren over de eOverheid zijn verschenen, ziet dat het verhogen van de effectiviteit en efficiëntie van het overheidsfunctioneren de belangrijkste motor achter de ontplooiing van de eOverheid is geweest (Snellen 2005: 399-400; Bekkers & Homburg 2009). De mantra 'meer met minder' is echter een riskante samenvatting van de metamorfose die overheidsorganisaties door ICT hebben ondergaan. Impliciet wordt daarmee veronachtzaamd dat ICT ook de overheid zelf heeft veranderd. De informatietechnologische overheid is niet, of niet alleen, een efficiëntere overheid, het is een *wezenlijk andere* overheid.

Veiligheid

Alhoewel anders van karakter dan effectiviteit en efficiëntie, vertegenwoordigt ook veiligheid een stuwend beginsel. Veiligheid is een dominant beleidsdoel in het huidige tijdsgewricht. Ook dit beginsel kenmerkt zich dus enerzijds door een grote mate van voordehandliggendheid – veiligheid is een bestaansreden van de staat –, maar anderzijds ook door een grote dynamiek en transformatie. Niet alleen

eist de dreiging van internationaal terrorisme veel politieke aandacht voor veiligheid op, ook de 'binnenlandse' behoefte aan veiligheid is sterk van karakter veranderd. Van de overheid wordt meer en meer verwacht dat zij risico's in kaart brengt en beheerst, bij voorkeur nog voordat deze zich voltrekken (Beck 1992; Boutellier 2003; WRR 2008b). Dit verwachtingspatroon vergt van de overheid een omschakeling van reactief naar proactief, van repressief naar preventief, van strafrecht naar integrale 'veiligheidszorg' (Johnston & Shearing 2003; Schinkel 2009).

ICT speelt een buitengewoon grote rol in deze omschakeling. De samenhang tussen ICT en de uitbouw van de controlesamenleving is bekend. Informatietechnologie heeft specifieke implicaties voor de registratie van het gedrag en handelen van burgers: observaties zijn intensiever, meeromvattend en indringender geworden. Bovendien blijven digitaal geregistreerde beelden en gegevens veel langer voorhanden dan wanneer de observatie door mensen (politieagenten, sociale rechercheurs, enz.) plaatsvindt. En eerder in dit hoofdstuk kwam al aan de orde dat digitalisering nieuwe mogelijkheden biedt voor toegang, uitwisseling en verrijking van informatie. Bezien vanuit het perspectief van opsporing, ordehandhaving en criminaliteitsbestrijding heeft de inzet van ICT daarom allerhande voordelen.

Veiligheid is als stuwend beginsel de motor achter vele ontwikkelingen en innovaties op het terrein van ICT en overheid. Het gaat hier echter niet om het neerzetten van een schrikbeeld (Big Brother). Wel kan uit het feit dat dergelijke schrikbeelden en doemscenario's regelmatig in publicaties en debatten opduiken worden afgeleid dat de initiatieven die in het belang van veiligheid worden ondernomen de neiging hebben om te expansief te zijn. Deze expansiedrang is ook waar te nemen bij andere vormen van controle die niet strikt genomen zijn ingegeven door veiligheidsbeleid. De sterk toegenomen aandacht voor handhaving van het recht en toetsing van rechtmatigheid, bijvoorbeeld met betrekking tot de publieke middelen die in de sociale zekerheid worden gestoken ('controle achter de voordeur'), is een exponent van dezelfde controle-impuls. Deze impuls is eveneens in hoge mate door ICT mogelijk gemaakt. Een concrete illustratie is automatische kentekenherkenning (ANPR - Automatic Number Plate Recognition). Behalve de politie, die deze cameratechniek inzet voor de handhaving van de openbare orde en opsporing van strafbare feiten, gebruikt de VROM-inspectie de gegevens voor controles van afvaltransporten, de Inspectie Verkeer en Waterstaat voor controle van het taxivervoer en controle op rij- en rusttijden, Rijkswaterstaat voor controle van verkeersstromen en de Belastingdienst voor controle op verschillende belastingen (Tweede Kamer 2009-2010j).

Het expansieve van de controlebehoefte uit zich in veel contexten als sluimerende *function creep*: het netwerkkarakter van informatietechnologie maakt het buitengewoon aantrekkelijk om aan allerhande systemen die in beginsel een andere func-

tie dienden een controlefunctie toe te voegen dan wel te verbinden met systemen die een controlefunctie hebben. Zo vroeg de CDA-fractie in de Eerste Kamer tijdens de behandeling van het wetsvoorstel voor invoering van het alcoholslot naar de relatie tussen enerzijds het systeem voor de registratie (bij het Centraal Bureau Rijvaardigheidsbewijzen (CBR) en de RDW) van alcoholmisbruik in het verkeer, en het Elektronisch Patiëntendossier anderzijds: "Voorziet de regering op termijn een link naar het Elektronisch Patiënten Dossier (EPD) vanwege de mogelijke relatie tussen alcoholgebruik, medicijngebruik en rijvaardigheid?" (Eerste Kamer 2009-2010d: 4). De technische mogelijkheden effenen het pad voor *function creep*.

2.4.2 VERANKERENDE BEGINSELEN

De individuele vrijheid van burgers, binnen de grenzen die daaraan in een democratische rechtsstaat gesteld kunnen worden, is van oudsher voortdurend onderwerp van discussie binnen de klassieke liberaal-democratische filosofie. De vrijheid van burgers om, binnen de grenzen van de wet, zichzelf te zijn, anders te zijn en dit anders-zijn openlijk te tonen en te verkondigen, is nauw verweven met burgerschap (Van Gunsteren 2009: 42). De collectieve en individuele kern van vrijheid waarin de overheid niet heeft te treden wordt gevormd door verankerende beginselen als de vrijheid van meningsuiting, nieuwsgaring en demonstratie, maar ook van keuzevrijheid en privacy. Deze verankerende beginselen fungeren als tegenwicht voor het technovertrouwen en het vaak overheersende belang van de hierboven besproken stuwende beginselen waarmee de introductie van applicaties bij de overheid gepaard gaat. Van deze verankerende beginselen worden in dit rapport keuzevrijheid en privacy onder de loep genomen, omdat juist de reikwijdte van deze twee belangen met de komst van ICT een belangrijk onderwerp van discussie vormt.

Zoals ten aanzien van de stuwende beginselen werd opgemerkt, is het van principieel belang dat de overheid de ruimte heeft om de kansen van ICT te benutten.[3] Tegelijkertijd echter moeten burgers beschermd worden tegen ongewenste implicaties daarvan. Die bescherming kan verschillende vormen aannemen. Het kan voorkomen dat de verankerende beginselen als absolute grenzen fungeren die zich verzetten tegen de introductie of een bepaald gebruik van een applicatie. Zo zou de overheid er bijvoorbeeld voor kunnen kiezen om de technologische mogelijkheid van gezichtsherkenning uit de handen van private partijen (bedrijven en burgers) te houden, vanwege potentieel ontwrichtende consequenties van een wijdverbreid gebruik. De verankerende beginselen kunnen ook grenzen stellen aan het koppelen van bepaalde systemen. Illustratief is het antwoord van de minister op de hiervoor geciteerde vraag van de CDA-fractie naar de koppeling tussen het EPD en de registratie van alcoholmisbruikers in het wegverkeer: "in een link tussen beide systemen wordt niet voorzien" (Eerste Kamer 2009-2010e: 12). Alhoewel hij

dat niet zo expliciet verwoordde, was de bijbehorende motivatie van de minister mede gestoeld op uitgangspunten van het privacyrecht.

In de bovengenoemde en andere situaties worden de verankerende beginselen betrokken in een afweging over de inzet van een applicatie. In de praktijk wordt die afweging gemaakt aan de hand van concrete gevallen. En in de juridische toetsing zijn beginselen als keuzevrijheid en privacy veelal niet meer dan zwaarwegende belangen: belangen die, zelfs al zijn ze reëel in geding, niet op voorhand de doorslag kunnen geven (vgl. Dworkin 1977). Ook in het maatschappelijke en politieke debat zijn de verankerende beginselen doorgaans geen alles-of-niets-concepten, maar fungeren zij als handvatten voor discussie.

Keuzevrijheid

Wie keuzevrijheid (of autonomie) bestudeert komt tot de conclusie dat dit verankerende beginsel overal en nergens in het recht aanwezig is. Overal, omdat het aloude (liberale) uitgangspunt 'alles is geoorloofd wat de wet niet verbiedt' nog steeds een belangrijke inspiratiebron voor de rechtsorde is. Nergens, omdat het tegelijkertijd geen waterdichte leidraad is voor burgers om hun handelen aan af te meten. Nergens wordt immers aan de orde gesteld wat die keuzevrijheid, zo belangrijk voor zowel de persoonlijke ontwikkeling van burgers als de conceptie van de rechtsstaat ('de vrije burger'), precies inhoudt of welke regeling er bestaat voor meer concrete gevallen. Bij wijze van uitzondering kent Duitsland een grondrecht op 'Algemeine Handlungsfreiheit' (bijv. Haratsch 2006), maar ook daar is deze klaroenstoot in de praktijk van weinig belang.

Het begrip 'keuzevrijheid' is voortdurend in beweging, niet in de laatste plaats vanwege innovaties in en toepassingen van ICT. Tegen onder meer de achtergrond van allerhande nieuwe media en daarop gebaseerde programma's en diensten kenmerkt de tegenwoordige tijd zich door een overdaad aan keuzes. Politiek-bestuurlijk krijgt de toename van keuzemogelijkheden bijvoorbeeld vorm door de liberalisering van de telecommunicatie en de zorg. Het burgerbeeld dat hierbij hoort, is dat van een geëmancipeerd individu dat, door zijn eigen koers uit te stippelen, bijdraagt aan het nut van het geheel. Een burger die optreedt als kritische consument werkt marktwerking en daarbij prijsverlaging immers in de hand. Kiezen is kortom een dure burgerplicht (Hurenkamp & Kremer 2005). Dit burgerbeeld past zeer goed bij de emanciperende mogelijkheden die ICT biedt. Keuzevrijheid is in die omstandigheden meer en meer ingevuld als informatievrijheid: de vrijheid om het eigen handelen te bepalen op grond van een ruim aanbod aan informatie en op informatie gebaseerde diensten (Lor & Britz 2007). Het is echter nog maar de vraag of mensen werkelijk zoveel behoefte hebben aan deze (verplichte) keuzevrijheid. Simon (1956) en later Schwartz (2004) hebben nadrukkelijk aan de orde gesteld dat een grote groep mensen hier weinig waarde aan hecht, dan wel niet zo goed in staat is keuzes te maken. Ook in de economische en sociaal-psychologische theorie is aandacht voor

de tekortkomingen van het zogenaamde 'rationele keuze model'. Gezien het feit dat dit perspectief op het gedrag van mensen veel wezenlijks buiten beeld houdt "is [het] beter om gewoon te accepteren dat de rationele keuzetheorie niet altijd even geschikt is om de wereld te begrijpen" (Tiemeijer 2009: 328). Kortom, keuzevrijheid is vandaag de dag een belangrijk maar ook nogal vluchtig thema.

Privacy

Privacy staat net als alle (klassieke) grondrechten voor een individuele sfeer van niet-bemoeienis door de overheid, maar ziet daarbij specifiek toe op de voorwaarden voor individuele menselijke ontplooiing. Privacy heeft een stevige grondrechtelijke status, die mede is gaan inhouden dat de overheid er garant voor moet staan dat dit recht ook tussen burgers onderling wordt gerespecteerd (bijv. Verhey 1992; Fredman 2008). Aan de eindverantwoordelijkheid van de overheid voor de bescherming van privacy kan dus niets worden afgedaan. Ook niet als deze verantwoordelijkheid moet worden waargemaakt tegen de achtergrond van een wereld waarin enorme private 'informatiemonopolisten' (Google, Amazon) de dienst uit lijken te maken en het internet nauwelijks te reguleren lijkt. Bovendien staan grondrechten in de dagelijkse realiteit in een spanningsvolle relatie tot elkaar, hetgeen nog eens versterkt doordat privacy inhoudelijk moeilijk af te bakenen is (vgl. Blok 2002; Solove 2008). Dit komt omdat privacy in de meeste situaties een afwegingskarakter heeft. En in de afweging delven de losse individuele belangen vaak het onderspit tegen de gepercipieerde belangen van het collectief. Het is dan ook niet eenvoudig om uit de concrete afwegingen die rechters omtrent privacy maken een kerninhoud van het recht te destilleren (bijv. Gómez-Arostegui 2005).

De lading van privacy is dan ook voortdurend in beweging, alleen al omdat opeenvolgende generaties van individuen er andere opvattingen over kunnen hebben. Zo lijkt de nieuwe 'generatie' *digital natives* (Palfrey & Gasser 2008) weer anders over privacy te denken (zie ook Boyd 2008) dan zij die nog 'de pre-internettijd' hebben meegemaakt. Veel belangstelling gaat momenteel uit naar de privacy van burgers ten opzichte van andere burgers, waarbij internettoepassingen als Facebook en Hyves laten zien dat de gebruikers voor de uitwerking van hun privacybescherming in toenemende mate afhankelijk zijn van aanbieders van deze diensten. Ook de opkomst van *cloud computing* is illustratief voor de ontwikkeling waarbij burgers in hun interactie met andere burgers en daarmee de uitoefening van hun privacy, meer en meer afhankelijk worden van grote (commerciële) spelers waarvan onbekend is waar ze zich bevinden en wie ze zijn. "What happens to your family's photo collection if it's held in the cloud and your password goes to the grave with you? And what about your documents and emails – all likewise stored in the cloud on someone else's server" (Naughton 2010a).

Privacybegrippen zijn echter altijd gevormd en aangepast in reactie op nieuwe technologieën, en het huidige tijdperk is daarop geen uitzondering. Zo vond het

Amerikaanse privacyrecht zijn oorsprong in de verspreiding van de technologie van de fotografie – of vormde daar eigenlijk een reactie op, met het fototoestel van de tabloidjournalist als belangrijk referentiepunt. In een beroemd geworden artikel bepleitten – en bewerkstelligden uiteindelijk – Warren en Brandeis (1890) een privacygrens die paal en perk moest stellen aan dit ongereguleerde en bedreigende fenomeen. De 'ruimte' die privacy waarborgt, is sindsdien steeds meer informationeel opgevat. Privacy is vanuit een traditionele fysieke functie (het huisrecht) geëvolueerd naar een meer immaterieel recht, waarin absolute grenzen veel minder makkelijk te trekken zijn (Floridi 2005). Tegelijkertijd met deze transformaties zijn er wel degelijk lijnen te trekken tussen het aloude fysiek begrepen huisrecht (*sanctity of the home*) en meer geestelijk begrepen vormen van moderne informationele privacy. Dat is namelijk de reële menselijke vereiste van enige mate van afzondering (voor individu of collectief), die nodig is om de persoonlijkheid te vormen, te ontwikkelen, en 'in de lucht te houden'. Met andere woorden, het belang een eigen identiteit te kunnen ontwikkelen en vormen. Hannah Arendt drukte het reële karakter van dit vereiste als volgt uit: "A life spent entirely in public, in the presence of others, becomes (...) shallow. [I]t loses the quality of rising into sight from some darker ground which must remain hidden if it is not to lose its depth in a very real, non-subjective sense" (geciteerd in Solove 2008: 164). Dat privacybegrippen worden gevormd en aangepast in reactie op nieuwe technologieën wordt nog eens geïllustreerd door de aanbeveling van de Staatscommissie Grondwet om privacy en persoonsgegevensbescherming op grondwettelijk niveau los te koppelen. Men kan stellen, aldus de Staatscommissie "dat – als gevolg van de technologische ontwikkelingen, Europese samenwerking en globalisering – de omvang van de uitwisseling en verwerking van persoonsgegevens de laatste jaren explosief is gestegen. Een verzelfstandiging van het recht op bescherming van persoonsgegevens geeft volgens de Staatscommissie uitdrukking aan de toegenomen betekenis van de verwerking van persoonsgegevens en de wenselijkheid van een behoorlijke bescherming in de huidige samenleving" (Staatscommissie Grondwet 2010: 81-82). Door alle aandacht voor gegevensverwerking in private relaties raakt de traditionele bescherming tegen de overheid met betrekking tot privacy en gegevensbescherming soms op de achtergrond (vgl. Levin & Sánchez Abril 2009). Dit maakt de uitdaging voor de overheid er echter niet minder op. Niet alleen vanwege de grenzen die getrokken moeten worden waar de overheid als gebruiker van ICT zelf de privacy van burgers inperkt, maar ook omdat zij toch niet aan haar eindverantwoordelijkheid kan ontkomen als het om de omgang met privacy in de informatiesamenleving gaat (De Hert 2011).

2.4.3 PROCESMATIGE BEGINSELEN

Ook als niet op voorhand is aan te geven hoe een afweging tussen de stuwende en verankerende beginselen zou moeten uitpakken, is er veel te zeggen over de kwaliteit van de randvoorwaarden van die afweging. De procesmatige beginselen – in

dit rapport uitgewerkt aan de hand van transparantie en accountability – bieden een kader dat de kwaliteit van de discussie en besluitvorming over de ontwikkeling van de elektronische overheid zeer ten goede kan komen. De procesmatige beginselen zijn van doorslaggevend belang voor de instandhouding van een goede balans tussen de stuwende en verankerende beginselen, maar ook voor het daaraan voorafgaande proces van zoeken en bediscussiëren van die balans. Ook dienen ze ter waarborging van de toetsbaarheid van het proces van ontwikkeling van de elektronische overheid. Transparantie en accountability tezamen eisen dat de vaak impliciete afwegingen die de overheid genoodzaakt is te maken bij de introductie van applicaties, inzichtelijk, navolgbaar en aanvechtbaar worden gemaakt.

De waarde van de procesmatige beginselen bestaat er enerzijds in dat op een macroniveau het discours van zowel de stuwende als van de verankerende krachten aan een *reality check* kan worden onderworpen, om zo op het niveau van de beleidsontwikkeling retoriek te scheiden van realiteit. Anderzijds hebben ze hun functie op een microniveau wanneer een beleidsuitkomst of concrete beslissing van een overheidsinstantie een individuele burger raakt. Via een goede invulling van deze beginselen, neergeslagen in institutionele arrangementen en regels, kunnen fouten worden rechtgezet en terugkoppelingsmechanismes ten behoeve van een lerende overheid worden ingebouwd.

Transparantie

Transparantie is voor burgers noodzakelijk om, ten eerste, het politieke en beleidsmatige proces te kunnen volgen en – eventueel – een tegenwicht te bieden en, ten tweede, om individuele rechten ten volle uit te kunnen oefenen. In veel opzichten gaat transparantie dan ook vooraf aan accountability.

Ten eerste is er een vorm van transparantie die de burger inzicht verschaft in beleidsprocessen, en zo de publieke ruimte van betere informatie voorziet. Deze vorm van transparantie heeft mede onder de noemer '(actieve) openbaarheid van bestuur' grote vooruitgang geboekt. Illustratief is bijvoorbeeld de *Open Government*-ambitie van de federale overheid in de VS, maar ook de diverse Nederlandse initiatieven variërend van internetconsultatie ten behoeve van wetgeving tot twitterberichten van politici en bestuurders. Voor burgers brengt het ontsluiten van dit soort informatie door middel van ICT vooral grote beloften en veel minder nadelen met zich mee. Niet alleen maakt deze transparantie het voor burgers mogelijk op de hoogte te blijven en politiek betrokken te zijn, het vormt ook de basis voor een rol als *countervailing power* ten opzichte van politiek en beleid.

De tweede vorm van transparantie is met name gericht op de situatie van het rechtzoekend individu. Hier is het soort transparantie nodig dat handvatten geeft voor individuele rechtsbescherming. Als een burger onbedoeld in de knel komt in de kluwen van een gedigitaliseerde overheid, dan zal hij of zij eerst inzicht moeten

krijgen in wat er gebeurd is, voordat er iets tegen in het werk gesteld kan worden. Vanwege de specifieke karakteristieken van informatietechnologie geldt hier vaak niet 'Wat niet weet, wat niet deert', maar eerder 'Wat niet weet, deert temeer'. Enige mate van transparantie in de interne processen van de dienstverlenende overheid is dus noodzakelijk om de positie van de burger te ondersteunen. Dat de overheid het potentieel van ICT ook daadwerkelijk – zij het schoorvoetend – benut voor deze transparantie aan individuele burgers blijkt wel uit webpagina's als mijn.overheid.nl, burgerpolis.nl en mijn.belastingdienst.nl. Belangrijk in dit verband is echter hoe ver transparantie als handvat voor (individuele) rechtsbescherming reikt. Zo dient zich in het licht van de soms zorgwekkende kwaliteit van overheidsinformatie (bijv. Grijpink 2006b; Choenni et al. 2011) en het groeiende probleem van identiteitsfraude de vraag aan wie de verantwoordelijkheid draagt om aan te tonen dat bepaalde informatie niet correct is en hoe deze persoon daar inzicht in kan krijgen. Een ander belangrijk aspect van de informatietechnologische volwassenwording van de overheid is dat tot op heden veel aandacht uitgaat naar de transparantie van de burger voor de overheid, en relatief weinig naar de omgekeerde relatie (Keymolen 2007; Prins 2007). Dit transparant maken van de burger (ten bate van proactief beleid, enz.) staat echter vooral in het teken van stuwende krachten als veiligheid en kan niet vereenzelvigd worden met het procesmatige beginsel transparantie.

Accountability

De notie accountability sluit nauw aan op de toetsbaarheid die door transparantie mogelijk wordt gemaakt, maar voegt daar bindende consequenties ('afrekening') aan toe. Accountability in zijn politieke vorm is – bijvoorbeeld via parlementaire controle en ministeriële verantwoordelijkheid – een belangrijk instrument voor het toetsen van de bevoegdheden van de overheid en de afwegingen die ze daarbij tussen de stuwende en verankerende beginselen heeft gemaakt. Accountability in zijn juridische vorm staat met name voor de mogelijkheden die de burger heeft om uitkomsten van de eOverheid aan te vechten. Als deze accountability voldoende is gewaarborgd heeft de burger niet alleen kans voor zijn individuele belangen op te komen. Er ontstaat ook, door de optelsom van acties van burgers, een kritisch tegenwicht dat behulpzaam kan zijn voor het versterken van de inhoudelijke kwaliteit van de relatie burger-overheid in het digitale tijdperk.

Naast deze meer publieke vormen van accountability heeft zich ook een organisatie-interne vorm ontwikkeld, die kan worden omschreven als 'accountability als managementcategorie'. Deze is vooral op controle en sturing (en leerprocessen) binnen organisaties gericht. ICT heeft het landschap op dit punt ingrijpend veranderd. Te denken valt aan de stroomlijning en sturing van het werk van professionals door zogenaamde expertsystemen, maar ook aan de enorme mogelijkheden voor de registratie van handelingen. Door op technisch niveau te *loggen* kunnen alle digitale handelingen worden geregistreerd en bewaard. Vervolgens kan aan

de hand van de managementinformatie die deze registraties opleveren worden gestuurd. Illustratief is in dit verband de reactie van de Vereniging van Nederlandse Gemeenten op het conceptwetsvoorstel voor de Verwijsindex Risicojongeren (VIR): "Mocht er op basis van meldingen in de VIR signalen binnenkomen dat een situatie met een jeugdige uit de hand loopt en de meldingsbevoegden nemen daarop, aangesproken door de regievoerder, hun verantwoordelijkheid niet of onvoldoende, dan moet helder zijn wie uiteindelijk de doorzettingsmacht heeft om zaken te regelen en hulpverleners een aanwijzing te geven" (VNG 2008: 2).

Het belang van accountability kan in deze tijd moeilijk overschat worden. Waar eenvoudige en eenduidige sturingsfilosofieën in de ogen van velen onvermijdelijk stuklopen op maatschappelijke complexiteit, biedt een procesbeginsel als accountability uitkomst. Het eist slechts een controlerelatie tussen een forum en een actor. Zo kunnen degenen wier belangen in het forum behartigd worden, vat krijgen op het opereren van de actor in kwestie. Deze nadruk op *operationele controle* onderscheidt het accountabilitymechanisme structureel van een 'oude kolos', het instituut wetgeving. Wetgeving is namelijk een poging om maatschappelijke verhoudingen en gedragingen van tevoren vast te leggen, terwijl 'verantwoording' naar de aard van het instrument toeziet op het daadwerkelijk functioneren, op de incidenten onderweg. Accountability, dientengevolge, "now crops up everywhere performing all manner of analytical and rhetorical tasks and carrying most of the major burdens of democratic 'governance'" (Mulgan 2000: 555).

2.4.4 AFWEGEN TROEF

Voor een evenwichtige ontwikkeling van de iOverheid is het van doorslaggevend belang dat elk van de 'clusters' van beginselen – stuwend, verankerend en procesmatig – bij besluitvorming voldoende gewicht wordt toegekend. Ze moeten tegen elkaar afgewogen worden, hoewel dat niet betekent dat ze allemaal en in elke situatie ook evenveel gewicht toegekend moeten krijgen. Maar dat impliceert tegelijk – omdat deze clusters meestal onderling op gespannen voet staan – dat er oog is voor de betrekkelijkheid van elk beginsel en elk cluster. Aan elk beginsel kan evengoed te veel als te weinig gewicht worden toegekend: de gevaren van dergelijke 'excessen' worden hierna in algemene lijnen geschetst. Het is kortom niet mogelijk om op voorhand aan te geven wat een 'goede' principiële afweging over ICT inhoudt, of hoe die uitpakt. Ook is, als in dit rapport wordt gesproken over een 'balans', niet geïmpliceerd dat los van de context kan worden voorgeschreven hoe die balans eruitziet. Maar dat laat onverlet dat er veel over afwegingen kan worden gezegd, en dat bijvoorbeeld kan worden geconstateerd dat de afwegingen in het (Nederlandse) politiek-bestuurlijke landschap vaak ontoereikend zijn, zoals in deel II zal blijken.

Stuwende beginselen, om daarmee te beginnen, zorgen goed voor zichzelf. In die zin hoeft men niet te vrezen voor een gebrek aan aandacht voor efficiëntie, effecti-

viteit en veiligheid. De overheid kan natuurlijk nooit een teveel aan efficiëntie of effectiviteit hebben, maar het denken in termen van die beginselen kan wel te dominant zijn. In dat geval worden alle overwegingen die men bij ICT in de relatie overheid-burger kan hebben, ingekapseld in een economische rationaliteit. Ook voor het beginsel veiligheid geldt dat de maatschappij er in principe nooit genoeg (laat staan te veel) van kan hebben, maar dat niettemin het denken wel te eenzijdig kan zijn. Een te ver doorgeschoten veiligheidsdenken zou veiligheid tegen elke prijs willen najagen. De 'prijs' van veiligheid kan echter een hoge zijn, en dan gaat het niet alleen om een economische afweging: in een samenleving waarin men zich niet meer onbespied weet, is het moeilijk om zichzelf te ontplooien. Het persoonlijke leven is "steeds meer een glazen huis waar nauwelijks gordijnen voor hangen" (Kohnstamm & Dubbeld 2007). Een te zwak ontwikkeld veiligheidsdenken daarentegen zou een overheid opleveren die zowel naïviteit kan worden verweten als het verzaken van zijn meest basale verantwoordelijkheid ten opzichte van burgers.

Zoals blijkt in deel II van dit rapport, worden de verankerende beginselen in het debat dikwijls overschaduwd door de stuwende beginselen. In het ontwikkelingsproces van een applicatie worden de verankerende beginselen niet vanzelfsprekend meegenomen. Ze vergen bijzondere aandacht en daadkrachtige pleitbezorgers. Toch geldt, net als voor de andere beginselen, ook voor keuzevrijheid (vgl. De Mul 2010) en privacy dat men er *te veel* van kan hebben. Zo zou een ongebreidelde keuzevrijheid van burgers om zelf te beslissen of hun persoonsgegevens worden verwerkt (bijvoorbeeld door opsporingsinstanties), uiteindelijk de veiligheid van andere burgers ondermijnen. En een overmaat aan keuze kan evengoed leiden tot keuzemoeheid waardoor men niet eens de moeite meer neemt een andere optie te overwegen of simpelweg maar wat aanvinkt. Maar ook van privacy kan een maatschappij te veel hebben: vrije burgers in een democratische rechtsstaat hebben ook plichten en dienen daartoe vindbaar en kenbaar te zijn. Privacybescherming heeft ook zijn risico's. In de beslotenheid van het privédomein kan zich immers veel onwenselijks afspelen: privacy kan bijvoorbeeld een voedingsbodem voor onveiligheid zijn. "In een rechtsstaat is het noodzakelijk dat personen die een inbreuk maken op de rechten van anderen, daarvoor ter verantwoording kunnen worden geroepen. Soms is het daarvoor bijvoorbeeld nodig dat de bestaande anonimiteit van een burger kan worden opgeheven en dat nader onderzoek kan worden verricht naar zijn activiteiten", aldus het kabinet-Balkenende IV (Tweede Kamer 2009-2010j: 12). Maar er is nog veel meer onwenselijks dat in de beslotenheid van de door het privacyrecht afgeschermde (fysieke dan wel geestelijke) cocon tot bloei kan komen. Criticasters van privacybescherming wijzen op overgeleverde (mannelijke) dominantiestructuren (Tadros 2006; Allen 2003), op geheimzinnigheid die schadelijk is in het economisch verkeer (Posner 1984) of op verstikking van publieke meningsvorming (Volokh 2000), en zelfs op armoede van geest in het algemeen (Kumar 2004).

Ook aan de procesmatige beginselen kan een excessief gewicht worden toegekend. Hoe belangrijk transparantie ook is, het kan niet als absolute eis worden gesteld. Om te beginnen zijn er zaken die te gevoelig liggen (vanwege privacy of staatsveiligheid) om openbaar te worden gemaakt. Bovendien verkeert transparantie in een complexe verhouding met vertrouwen in de overheid. Weliswaar kan de overheid transparantie inzetten om vertrouwen te stimuleren (Keymolen et al. 2011; Van der Hof & Keymolen 2010), maar er kan evengoed sprake zijn van een overdaad aan transparantie ten koste van vertrouwen (Luhmann 1979). Transparantie als instrument van de overheid (Fung, Graham & Weil 2007) kan bovendien manipulatief zijn als de prijsgegeven informatie nooit in een daarvoor geschikt forum wordt getoetst (Meijer, Brandsma & Grimmelikhuijsen 2010). Dat een maatschappij ook van accountability te veel kan hebben is alleen al af te leiden uit de klank van de term *audit explosion* (Power 2005). Een teveel aan accountability kan ten koste gaan van slagvaardigheid (effectiviteit en efficiëntie) en van creativiteit (innovatie).

2.5 TOT SLOT

Het hiervoor gepresenteerde analysekader, de nadere theoretische duiding van de centrale thema's en de driedeling in beginselen dienen als zoeklichten voor de in deel II gepresenteerde analyse van de praktijk en de realiteit van de eOverheid. Deze realiteit toont een overheid die onder invloed van digitalisering ingrijpend van karakter is veranderd. De facto en bijna ongemerkt blijkt zich een praktijk te ontwikkelen, waarin samenhangende informatiestromen het karakter van de overheid domineren. Deze praktijk blijkt echter niet op het netvlies van politiek en beleid te staan, waardoor er allesbehalve vanuit het samenhangende idee van snel groeiende en vertakkende informatiestromen wordt gedacht en gewerkt. Ondertussen stroomt meer en meer informatie tussen verschillende organisaties, tussen voorheen onderscheidende terreinen (service, care en control) en over publiek-private grenzen heen. De empirische analyse in deel II volgt het pad van de informatiestromen in plaats van de individuele techniek en de losse applicaties, en laat zien dat in empirische zin een iOverheid 'ontstaat' zonder dat deze op politiek-bestuurlijk niveau 'ontworpen' is.

NOTEN

1 Zie https://www.bof.nl/2010/09/22/geen-openheid-over-nederlandse-blokkade-verboden-websites/

2 Mede omvattende werk & inkomen, belastingen en douane, onderwijs, verkeer & vervoer, enz.

3 En ook om de benutting van die kansen in de maatschappij (markt) niet nodeloos te hinderen.

DEEL II

DE EMPIRISCHE ANALYSE

3 DE AANSTURING VAN DE eOVERHEID

In het voorgaande hoofdstuk is uiteengezet dat de aandacht in dit rapport niet zozeer uitgaat naar individuele technologieën of naar technologie in het algemeen, maar naar de technologische systemen in relatie met hun omgeving. Deze socio-technologische systemen behelzen complexe netwerken van mensen, technologische applicaties, (overheids)organisaties en bedrijven. Drijfveren, belangen en motieven van betrokken actoren spelen een belangrijke rol in het bepalen van de richting van de technologieontwikkeling en in het genereren en benutten van informatie. De interactie en wisselwerking binnen dit socio-technologisch systeem vormt dan ook het vertrekpunt voor de analyse in dit empirische deel van het rapport. Deze analyse zoomt in op de relaties tussen de belangrijke spelers die de eOverheid vormgeven en laat zien hoe besluiten van deze spelers over de inzet van technologie en het gebruik van informatie tot stand komen, hoe afwegingen worden gemaakt en beargumenteerd en welke rol ieder van de betrokken actoren daarin speelt. Deze positioneringen worden vervolgens geduid vanuit de in het voorgaande hoofdstuk geïntroduceerde stuwende, verankerende en procesmatige beginselen. Bij de analyse van interacties zal niet alleen langs de band van technologische applicaties worden gekeken. De blik zal zich vooral richten op de informatiestromen die door de technologie zijn ontstaan of erdoor zijn gefaciliteerd. Juist op het niveau van informatiestromen vervloeien de – toch al niet scherp afgebakende – randen tussen verschillende beleidsterreinen, kolommen, sectoren en de spelers die daar actief zijn. Door deze focus op informatiestromen worden de contouren zichtbaar van de stille revolutie in de eOverheid die de toekomst en het gezicht van de overheid in het digitale tijdperk sterk zal gaan bepalen.

3.1 POLITIEK-BESTUURLIJK ENTHOUSIASME EN VERTROUWEN

3.1.1 DE GEESTEN RIJP

Aan de vooravond van de aanslagen in New York, op 21 juni 2001, vond een tussentijds Algemeen Overleg plaats tussen de Tweede Kamer en de minister van Binnenlandse Zaken. Aanleiding vormde de brief van de minister over de noodzaak tot opname van een biometrisch kenmerk in reisdocumenten en een recent werkbezoek van enkele Kamerleden aan de makers van het paspoort, Johan Enschedé en de Sdu. De teneur van de discussie was een onder alle partijen, zowel minister als Kamerleden, breed gedragen enthousiasme.

"De heer Zijlstra (PvdA) toont zich na een bezoek aan Johan Enschede en de Sdu zeer onder de indruk van de geavanceerde ontwikkelingen en vele mogelijkheden op het terrein van de biometrie. (...) De heer De Swart (VVD) is na een bezoek aan Johan Enschede en de Sdu ook onder de

indruk van de mogelijkheden met biometrie. Met name de vingerscan en irisscan zijn al behoorlijk ver in ontwikkeling. (…) Misschien moet Nederland overwegen een voortrekkersrol te vervullen en vooruitlopend op andere Europese landen biometrische kenmerken invoeren. (…) De heer Balkenende (CDA) constateert, na zijn bezoek aan de Sdu en Johan Enschede, dat het indrukwekkend is om te zien wat er technisch allemaal kan en gebeurt. (…) De CDA-fractie vindt het opnemen van biometrische kenmerken (…) urgent en dringt aan op spoed. (…) De heer Balkenende constateert dat het opnemen van een biometrisch kenmerk wijziging van artikel 3 van de Paspoortwet noodzakelijk maakt. Dit is een technische verbetering, geen principiële wijziging (…)" (Tweede Kamer 2000-2001a: 1-3).[1]

De passages uit het verslag van het Algemeen Overleg zijn illustratief voor de houding die beleid en politiek het afgelopen decennium hebben aangenomen ten opzichte van ICT. Deze houding wordt gekleurd door a) een groot enthousiasme en welhaast absoluut vertrouwen in ICT en b) een vaak instrumentele visie op wat ICT is en kan. De beleidsplannen die vanaf begin jaren negentig het licht zagen, ademen allemaal een groot vertrouwen in ICT als middel om effectiever, klantvriendelijker, toegankelijker, kwalitatief beter en beter voorbereid op de toekomst de taken van de overheid uit te voeren (zie bijv. ministerie van EZ 1994; ministerie van BZK 1998; ministerie van BZK 2000; ministerie van Sociale Zaken en Werkgelegenheid (SZW) 2010). Zowel in het licht van de grootse administratieve opdracht waar de overheid voor staat als bij de aanpak van urgente maatschappelijke uitdagingen als terrorisme, veiligheid, mobiliteit, en goede en betaalbare zorg, is ICT enthousiast binnengehaald door de (Nederlandse) politiek. Het inzetten van technologie wordt bijna als een vanzelfsprekendheid gezien. Tekenend zijn de mededelingen van toenmalig minister van Volksgezondheid, Welzijn en Sport (VWS) Hoogervorst, in een tweetal brieven aan de Tweede Kamer over het landelijk Elektronisch Patiëntendossier.

"Ik ben in deze brief niet meer ingegaan op de noodzaak van de invoering van het Elektronisch Medisch Dossier (EMD) en het EPD. Iedereen is er immers van overtuigd dat deze ontwikkeling zo snel mogelijk tot stand moet komen" (Tweede Kamer 2004-2005: 8).

En:

"Een tweede conclusie is dat het geen twijfel leidt dat door de invoering van het waarneemdossier huisartsen en het elektronisch medicatiedossier de kwaliteit van zorg zal verbeteren" (Tweede Kamer 2006-2007: 4).

Technologie wordt 'uitgerold', praktijken worden 'gestroomlijnd' en diensten 'geüpdatet'. Zo realiseren de ICT-applicaties ontwikkeld binnen het Programma Vernieuwing Grensmanagement van het ministerie van Veiligheid en Justitie dat in het grenstoezicht sprake is van een goede balans tussen het controle- en veiligheidsbelang en het economisch belang van Nederland bij een vlotte en klantgerichte afhandeling van personen- en goederenstromen.[2] Ook in de nota *Contract met de toekomst, een visie op de elektronische relatie overheid-burger* (Ministerie van BZK 2000) wordt veel verwacht van het probleemoplossende vermogen van ICT.

"ICT is meer dan alleen een handig hulpmiddel voor verbetering van de efficiency. Als ICT goed wordt benut kan het een belangrijke bijdrage leveren aan de beleidsdoelstellingen van een sector. Het kan de justitiële keten soepeler laten functioneren, zoals dat ook bij de Belastingdienst het geval is. Het kan in het onderwijs een alternatief zijn voor tekorten aan leraren en remedial teachers, de kwaliteit van het bestaan van ouderen aanmerkelijk verbeteren en de veiligheid op straat fors verhogen. Die mogelijkheden zijn er al, maar moeten nog worden gerealiseerd. Voor een goed inzicht van de mogelijkheden van ICT binnen een sector zijn de deskundigen uit die sector nodig. Zij hebben voldoende kennis van het primaire proces om te bedenken welke bijdrage ICT daaraan zou kunnen bieden. Het is dus van belang in de sectoren een denkproces op gang te brengen over de probleem-oplossende werking van ICT" (Ministerie van BZK 2000: 23).

3.1.2 VAN DIENSTVERLENING TOT ZORG EN CONTROLE

De aantrekkingskracht van nieuwe technologische innovaties lag in eerste instantie primair op het terrein van de dienstverlening. Een eOverheid is "een overheid waarbij het verkeer tussen overheid en burger zo veel mogelijk langs elektronische weg plaatsvindt, met als doel betere dienstverlening, betere handhaving en bevordering van inspraak en zeggenschap. (…) het belang van de burger is hierbij het uitgangspunt" (Commissie-Postma-Wallage 2007: 4). Met een dergelijke ambitie in het achterhoofd sloeg de Nederlandse politiek in de jaren tachtig en negentig de weg van de digitalisering in. De mogelijkheden om het beleid te verbeteren, om meer met minder te doen en om het handelen van de overheid ten opzichte van de burger beter, sneller en efficiënter te laten verlopen, werden gezocht in een enthousiaste digitalisering van administratieve processen en aansprekende projecten als de Burger Service Kaart en het Overheidsloket 2000 (Van de Donk & Meyer 1994; Huydecoper et al. 2001; Bekkers et al. 2005; Van de Donk & Van Dael 2005). Toch concludeerde de Raad voor het openbaar bestuur (Rob) in 1998 naar aanleiding van een adviesaanvraag van de minister van Binnenlandse Zaken, dat vele kansen om ICT in te zetten ter verbetering van de dienstverlening aan de burger nog onbenut bleven. De projecten die zijn gestart in het kader van het project Overheidsloket 2000 moeten volgens de Rob worden gezien "als vingeroefeningen voor het grote werk dat nog moet gaan beginnen" (Rob 1998: 23).

Met dat grote werk maakten bestuur en politiek enkele jaren later daadwerkelijk een aanvang. In de hiervoor al geciteerde nota *Contract met de toekomst* (Ministerie van BZK 2000) formuleerde het kabinet een ambitieuze agenda om met behulp van ICT zowel de eigen gegevenshuishouding als de dienstverlening aan burgers te verbeteren. Waar in de begindagen van de eOverheid de meeste aandacht nog uitging naar het poneren van een visie op een 'nieuwe overheid', worden de ambities nu (veelal sterk top-down) uitgewerkt in concrete programma's en convenanten zoals het in december 2008 ondertekende akkoord *Nationaal uitvoeringsprogramma betere dienstverlening en e-overheid* (NUP). Het NUP is een akkoord van rijk, provincie, waterschappen en gemeenten gericht op betere dienstverlening met minder administratieve lasten. "Om dat te bereiken moeten overheden (nog) meer samenwerken, hun bedrijfsvoering en gegevenshuishouding op elkaar afstemmen en aansluiten op reeds ontwikkelde en nog te ontwikkelen basisvoorzieningen."[3] Die gedachte resulteerde de afgelopen tien jaar in een diversiteit aan plannen en concrete initiatieven: de invoering van een Burgerservicenummer (BSN), de modernisering van de gemeentelijke basisadministratie persoonsgegevens (GBA) en diverse andere basisadministraties, de verdere uitbouw van de intermediaire organisatie voor elektronische gegevensuitwisseling tussen overheidsinstanties (RINIS), de instelling van één digitaal klantcontactpunt voor inkomensondersteunende voorzieningen en vele voorzieningen voor bestuursrechtelijke rechtshandelingen (aanvragen van vergunningen, indienen van bezwaarschriften).[4] Niet alleen deze, maar ook de vele andere initiatieven hebben de dienstverlening van de overheid in diverse opzichten veranderd (zoals continue beschikbaarheid, interactiever) en soms ook daadwerkelijk verbeterd. De tijd om de successen te vieren lijkt echter over het algemeen vrij kort: verbeteringen in de dienstverlening worden al heel snel als 'gewoon' ervaren en nog nauwelijks als een prestatie geregistreerd. De 'stille' successen bij gemeenten en vele uitvoeringsdiensten worden veelal overschaduwd door de meer in het oog lopende grote en dure projecten die geplaagd worden door vertragingen en mislukkingen.

Het grote werk dat de Rob aankondigde toont zich niet alleen op het terrein van de dienstverlening. Het afgelopen decennium kreeg 'Den Haag' meer en meer aandacht voor technologie als oplossing voor nijpende maatschappelijke problemen. Dat had veel te maken met zowel het vertrouwen dat technologie een goed instrument is om efficiënter en effectiever te kunnen werken bij de aanpak van deze problemen als de politieke aandacht voor vraagstukken van sociale veiligheid tot nationale veiligheid, waarin technologie een steeds grotere rol wordt toebedeeld. Voor beide ontwikkelingen geldt dat Nederland daarin beslist niet alleen staat (Lyon 2007; Dunleavy et al. 2006; Monahan 2006; Zureik & Salter 2005; Bennett 2008; Magnet 2009). Met name op het gebied van de sociale veiligheid is de digitalisering in het beleid de afgelopen jaren sterk toegenomen: camera's waken over de veiligheid op straat, de Verwijsindex Risicojongeren (VIR) en het Elektronisch Kinddossier (EKD) moeten risico's voor kinderen en jongeren signa-

leren en tijdig ingrijpen mogelijk maken, en databanken met vingerafdrukken en DNA-codes maken opsporing eenvoudiger. Op het gebied van de nationale veiligheid geldt welhaast een technologisch imperatief: de dataverzameling in het kader van de veiligheid heeft ongekende proporties aangenomen. Zo vroegen opsporingsdiensten in 2009 bijna 3 miljoen keer (2.930.941 keer) bij telecombedrijven en internetproviders gegevens van klanten op (CIOT 2010a). Bovendien bleek uit het – na een Wob-verzoek openbaar gemaakte – Eindrapport van de Audit CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie) dat medewerkers van bijzondere opsporingsinstanties deze gegevens zonder de benodigde toestemming van de officier van justitie opvragen (CIOT 2010b). Over de exacte omvang van vele andere verzamelingen blijft het echter gissen: “Iedereen constateert dat de bevragingen in de afgelopen jaren sterk zijn gegroeid, maar een cijfermatige onderbouwing daarvan kan alleen op onderdelen worden verkregen” (Adviescommissie Informatiestromen Veiligheid 2007: 66).

3.1.3 GEDREVEN DOOR AMBITIE

Niet alleen overheerst in politiek en beleid een groot enthousiasme en vertrouwen waar het de inzet van ICT betreft. De ambities zijn ook groot. Aan politieke zijde is volgens de Algemene Rekenkamer (2007a) sprake van een ‘ICT-enthousiasme’ van bestuurders, onrealistische politieke deadlines en onvoldoende gelegenheid tot heroverwegingen gedurende de projecten. ICT-projecten bij de rijksoverheid zijn volgens de Algemene Rekenkamer te ambitieus en complex door een continue spanning tussen de politieke, organisatorische en technische factoren van een project. De Rijks-Chief Information Officer (CIO, zie ook par. 6.3) Hillenaar wijst ook op de neiging van de overheid (niet alleen de Nederlandse) om grote projecten te ambiëren, waarbij *fantasy deadlines* – om de zaak bijvoorbeeld binnen een regeerperiode tot stand te brengen – en de neiging om veel zelf te willen bouwen ervoor zorgen dat fouten steeds weer opnieuw worden gemaakt. Ook heeft de politiek regelmatig de neiging om tussentijdse wijzigingen door te voeren en daarmee de scope van het project te beïnvloeden.[5] Bovendien ontstaat rondom grote projecten vaak een politieke ‘alles of niets’ dynamiek: van de zijde van de regering geldt dat grote projecten niet mogen mislukken of zelfs maar vertraagd raken. Zo brachten de 330.000 bezwaren tegen het EPD – een aantal dat medio 2010 met nog eens ruim 100.000 was toegenomen en geen precedent heeft – minister Klink in december 2008 niet verder dan de opmerking dat dit ‘spoort met het aantal dat hij verwacht had’ (Pluut 2010: 21).

Maar de grote ambities tonen zich niet alleen in de omvang en complexiteit van de projecten. Ambitieus zijn de plannen ook in beleidsinhoudelijke zin. Vanuit de politieke opdracht om de veiligheid van burgers te waarborgen, en vanuit het vertrouwen in technologie om die klus te klaren, ontstaat de ambitie om de toekomst in kaart te brengen en daar alvast op te anticiperen. “Het technische

systeem moet de onbehaaglijke onzekerheid uitbannen" (Hirsch Ballin 1992: 77). Vanuit de gedachte dat voorkomen altijd beter is dan genezen stelt ICT de overheid nu daadwerkelijk in staat om proactief en preventief te handelen (Schinkel 2009). De VIR moet voorkomen dat er een nieuw Maasmeisje sterft, het EPD moet medische missers voorkomen, Europese migratiedatabanken moeten voorkomen dat nieuwe illegalen zich in Nederland vestigen, en opsporingsdatabanken en de uitwisseling van Passenger Name Records (PNR)-data, bankgegevens en DNA-gegevens moeten een nieuwe terroristische aanslag voorkomen. De politiek-bestuurlijke neiging om een voorschot op de toekomst te nemen leidt tot fundamentele paradigmaverschuivingen. Zo schuift het doel en het bereik van het strafrecht op van reactie, vergelding en rehabilitatie naar preventie en risicobeheersing: de *pre-crime logic of security* (Zedner 2007; Koops 2006; Teeuw & Vedder 2008; Buruma 2011). Garland (2001) spreekt van een *culture of control* en schetst een politiek klimaat waarin bij de criminaliteitsbestrijding de aandacht niet langer uitgaat naar resocialisatie van burgers die ongewenst gedrag vertonen. Centraal staat nu de ambitie om burgers die normconform handelen te beschermen tegen individuen die zich afwijkend gedragen.

3.1.4 EEN VOOR EEN STAPELEN

Gedreven door zowel enthousiasme voor als vertrouwen in de mogelijkheden van technologie, de ambitie om met behulp van ICT maatschappelijke uitdagingen aan te pakken en voortgestuwd door beginselen als veiligheid en effectiviteit & efficiëntie, liggen in de politieke praktijk niet alleen de inzet van losse applicaties voor de hand, maar ook de mogelijkheden voor koppeling en uitwisseling van informatie. Als een koppeling van informatiesystemen tussen Belastingdienst en UWV fraude aan het licht brengt, dan moet daar ruimte voor zijn. Als een kind gered kan worden door zoveel mogelijk organisaties toegang te geven tot het Elektronisch Kinddossier, dan moet dat overwogen worden. Als de vingerafdrukken van asielzoekers die in het kader van het migratiebeleid zijn verzameld ook gebruikt kunnen worden voor opsporing, wat is daar op tegen? Als de grensoverschrijdende uitwisseling van DNA-gegevens efficiënter kan plaatsvinden door nationale databanken wederzijds voor elkaar toegankelijk te maken, dan ondertekenen we daartoe een verdrag. Als het verspreiden van kinderporno kan worden tegengegaan door al het internetverkeer op inhoud te screenen via zogenaamde *deep packet inspection* (DPI), dan moet die optie serieus worden overwogen.

Wie kijkt naar de groeiende aandacht voor het koppelen van systemen en databanken, ziet dat, alhoewel technologie het politieke debat beheerst, het eigenlijk gaat om de informatiestromen die door de verschillende technologieën mogelijk worden gemaakt. Informatie is de grondstof voor preventief beleid, omdat de profielen waarop risicoanalyses en preventie zijn gebaseerd alleen met behulp van (persoons)informatie zijn samen te stellen (Harcourt 2007; Hildebrandt &

Gutwirth 2008; Buruma 2011). Zo ook is informatie de primaire grondstof wanneer in het kader van 'dienstverlenend' armoedebeleid bepaalde groepen burgers proactief hun gemeente- of waterschapsbelasting kan worden kwijtgescholden of voorzieningen in het kader van bijzondere bijstand kunnen worden geboden (Tweede Kamer 2009-2010b). Vaak ook winkelt de overheid voor de benodigde informatie in de gegevensverzamelingen in het private domein.
In toenemende mate verlangt de overheid dat gegevens die in de private sector primair voor commerciële dienstverlening zijn verzameld, aan de overheid worden verstrekt. Waarbij deze gegevens dan niet voor service, maar ten behoeve van control worden ingezet. Berkvens (1992) sprak in dit verband al eerder over nieuwe 'Heerendiensten' in het digitale domein. Het afgelopen decennium zijn alleen maar meer wetten geïntroduceerd die deze mogelijkheden faciliteren, zoals de Wet vorderen gegevens, Wet bewaren verkeers- en locatiegegevens en Europese regelingen voor de doorgifte van passagiersgegevens en bancaire (SWIFT) gegevens aan de VS. Maar naast publiek-private informatiestromen die door speciale wetten worden gelegitimeerd, blijkt er ook veel mogelijk door afstemming van onderaf. Als bijvoorbeeld een gemeentelijke Sociale Dienst fraude bij uitkeringen op het spoor wil komen, dan staat de Wet bescherming persoonsgegevens (WBP) in principe toe dat een bestandskoppeling met bijvoorbeeld het waterleidingbedrijf wordt gemaakt (CBP 2006: 1). In al deze gevallen lopen door gestapeld gebruik van informatie, service (in dit geval van de private sector) en control (publieke sector) in elkaar over. Andersom lift de private sector ook graag mee met de overheid: "VNO-NCW is verontrust over de tot nu toe gemiste kans om het wetsvoorstel inzake het Burgerservicenummer (BSN) ook van nut te laten zijn in de ondernemingsadministratie" (VNO-NCW 2005). En bij de beoordeling van de subsidieaanvraag van de Immigratie- en Naturalisatiedienst voor geautomatiseerde grenspassage (No-Q) concludeerde Het Expertise Centrum (HEC): "Het realiteitsgehalte van de doelstellingen is onderbouwd door stevig commitment van zowel overheid als private partij Schiphol."[6]

De politieke aandacht richt zich in de regel echter niet op de interactie van allerhande applicaties en informatiestromen, maar op een individueel initiatief, en bespreekt die als opzichzelfstaand. Zo worden debatten gevoerd over het biometrisch paspoort, de OV-chipkaart, het BSN, DigiD, het digitaal klant dossier (DKD), het elektronisch leerdossier (ELD), het Elektronisch Patiëntendossier (EPD), de Verwijsindex Risicojongeren (VIR) en de Persoonlijke Internet Pagina (PIP). De concrete, voorliggende applicatie bepaalt het debat. Al naar gelang de dynamiek die zich in het politieke debat ontwikkelt, vernauwt de focus zelfs naar een deelaspect daarvan: zo ging het debat over de OV-chipkaart met name over de 'kraakbaarheid' van de chip (Van Eeten 2011). Toenmalig minister van BZK Ter Horst, gevraagd naar de tegenslagen bij de invoering van de Rijkspas, verwoordde deze versmalling indirect door te stellen: "Elke keer worden wij weer geconfronteerd met berichten dat het mogelijk is dat de technologie niet zo veilig is als gedacht en

gehoopt, dus elke keer moeten dan opnieuw maatregelen worden genomen" (Tweede Kamer 2008-2009c: 3). Het achterliggende netwerk van informatiebelangen en informatierelaties dat ontstaat, dan wel zich verder vertakt, blijft in de regel buiten het publieke en politieke debat. De onderlinge samenhang, de koppelingen en keteninformatisering die achter individuele applicaties schuilgaan en in de uitvoeringspraktijk stap voor stap vorm krijgen, blijven veelal onbesproken. Waar op het niveau van de applicaties veelal nog wel de parlementaire weg wordt bewandeld (zij het soms laat in het proces, zoals bij het EPD en de VIR), is dit bij koppelingen tussen systemen (als onderscheiden van applicaties) nauwelijks het geval. Veel van deze koppelingen worden gelegitimeerd via het ruime regime van de Wet bescherming persoonsgegevens (WBP), waardoor beslissingen over koppelingen vrijwel nooit openlijk en op politiek niveau worden bediscussieerd. De 'toets' blijft beperkt tot een melding conform de WBP bij het College Bescherming Persoonsgegevens (CBP), waarbij dergelijke meldingen slechts in uitzonderingsgevallen aanleiding vormen tot een kritische blik van het College. Een zoektocht in het (online raadpleegbare) meldingenregister van het CBP toont de rijkdom aan koppelingen, met name op uitvoeringsniveau en binnen gemeenten, die inmiddels vrijwel volledig onttrokken aan zichtbare controle en debat is ontstaan.

De neiging om steeds meer informatie te verzamelen, terwijl het politieke debat zich vaak beperkt tot de voorliggende applicatie en het bijbehorende wetsvoorstel, maakt dat koppelingen en de informatiestromen die daaruit resulteren ook steeds breder zijn en verknoopter raken. Informatie die is verzameld onder de noemer van dienstverlening, zorg of veiligheid (*service, care* of *control*) wordt in toenemende mate ook buiten die context gebruikt, gekoppeld en verwerkt. Tekenend voor het combineren van systemen die in eerste instantie op dienstverlening waren gericht en nu ook ten behoeve van controle en handhaving worden ingezet, is het initiatief van de minister van Justitie tot het opzetten van een landelijk register met gegevens van prostituees, met gebruikmaking van de GBA.[7] Doordat de Naam, Adres, Woonplaats (NAW) gegevens voor deze databank worden opgevraagd, komt in de GBA een aantekening dat gegevens over de betreffende persoon zijn verstrekt voor deze prostitutiedatabank. Omdat uit de GBA niets kan worden verwijderd (het systeem overschrijft bij wijziging niet, maar vult de gegevens met een nieuwe aantekening aan), is voor een ambtenaar burgerzaken, die zich primair richt op dienstverlening aan burgers, niet alleen zichtbaar dat betreffende persoon prostituee is, maar zal ook voor de toekomst altijd zichtbaar blijven dat die persoon ooit prostituee is geweest. De verderstrekkende consequenties van de aangroeiende stapel van contextoverstijgend met elkaar verbonden applicaties worden in zowel beleid als politiek niet geadresseerd. En daar waar het parlement in een enkel geval opmerkt dat een initiatief "verderstrekkende gevolgen heeft c.q. kan hebben dan zo op het eerste gezicht met de invoering ervan werd beoogd" (Eerste Kamer 2006-2007: 1), blijft een reactie vanuit het verantwoordelijk departement over het algemeen uit.

3.1.5 SPAARZAAM KRITISCH

Dat wil overigens niet zeggen dat de inbreng van het parlement als onbetekenend bestempeld moet worden. Beide Kamers, maar in het bijzonder de Eerste Kamer, hebben zich meermalen een kritisch opponent van regeringsambities getoond. Soms werd het kabinet er zelfs van beticht het parlement op voorhand buiten spel te zetten door zaken als toetsingskader en criteria voor de inzet van een applicatie niet in de wet maar in een Algemene Maatregel van Bestuur op te nemen, zoals bij de introductie van het BSN (Eerste Kamer 2006-2007: 1-2). In de kritische opstelling vindt het parlement soms de helpende hand van burgerbewegingen en maatschappelijke organisaties (zie par. 7.2), doordat deze op een groeiend aantal dossiers een bijdrage leveren aan het scherp houden van het democratisch toezicht (Eijkman 2010; Prins 2010a). Ook het Rathenau Instituut leverde via meerdere Berichten aan het Parlement en andere studies een bijdrage aan de politieke oordeelsvorming (Rathenau 1998; Rathenau 2008: 18; Rathenau 2010: 18-19). Met name de Eerste Kamer heeft zich gevoelig betoond voor dit soort inbreng, en is bij een aantal dossiers tot een ander oordeel gekomen dan de Tweede Kamer. Zo speelde de Consumentenbond een belangrijke rol bij het verwerpen van het wetsvoorstel over de slimme energiemeter door de Eerste Kamer, begin april 2009 (Eerste Kamer 2008-2009a; Cuijpers en Koops 2009). Ook bracht de Eerste Kamer de zwaar bekritiseerde bewaartermijn (onder meer CBP 2007) voor dataretentie, dat wil zeggen de termijn waarbinnen onder meer Internet Service Providers (ISP's) de 'verkeersgegevens' van hun klanten moeten bewaren, terug van de 12 maanden die de Tweede Kamer had goedgekeurd naar een maximum van 6 maanden. De Tweede Kamer had deze zelf al teruggebracht van de 18 maanden die door de regering waren voorgesteld. Ook het EPD-dossier bleek dusdanig complex dat de Eerste Kamer zijn bijnaam van *Chambre de reflection* extra heeft opgetuigd door middel van het beleggen van een aantal expertsessies om zich te informeren en de eigen oordeelsvorming te verbeteren. En ten slotte besloot de Eerste Kamer om in mei 2011 in aanwezigheid van de verantwoordelijk bewindspersonen een beleidsdebat te houden over "privacy, digitale dataopslag en data uitwisseling" (Eerste Kamer 2010-2011).

Toch lijkt de meerderheid van de ontwikkelingen en voorstellen aangaande ICT en informatiesystemen zich bijna ongezien door het democratisch bestel te bewegen en dat is in feite al jaren zo (zie bijv. Snellen 1992). Wanneer de toepassingen opzien baren is dat vaak pas op het moment dat de kogel eigenlijk al door de kerk is. De invoering van het biometrisch paspoort en met name de opslag van de vingerafdrukken in een centrale databank heeft bijzonder weinig publieke en politieke aandacht gekregen tot het moment dat deze door de Eerste Kamer goedgekeurd zou worden (Böhre 2010; Snijder 2010). Pas toen ontstond er nog wat maatschappelijke reuring aangevoerd door enkele ngo's en wetenschappers. Leden van de Eerste Kamer gaven in gesprekken met de WRR aan dit dossier achteraf gezien

onvoldoende scherp gevolgd te hebben.[8] Tweede Kamerfracties die eerder de regeringsplannen steunden, tonen zich nu alsnog bezorgd.

"Er zijn reële risico's: fraude, function creep en verkeerd gebruik (...) Het is en blijft mij dan ook volstrekt onduidelijk waarom wij in Nederland zo nodig het voortouw hebben willen nemen en twee doelen in één wet hebben willen verenigen, namelijk het bestrijden van identiteitsfraude – een doel waar ik mij volledig in herken en wat ik ook wil – maar ook het opsporen van strafbare feiten, en dan met die database als verbindende factor", aldus VVD-Kamerlid Hennis-Plasschaert (Tweede Kamer 2010-2011a: 4).

Maar een goede en toekomstgerichte democratische controle is geen eenvoudige opgave en blijkt voor veel politici lastig, zo bleek uit gesprekken met diverse Kamerleden. Dit is zeker het geval wanneer plannen op Europees niveau tot ontwikkeling komen, zoals bij Frontex (de EU Border Management Agency) en het voorgenomen Europese Entry/Exitsysteem, aldus Eerste Kamerlid Meurs.[9] Leden van de Tweede en Eerste Kamer geven aan dat zij, vanuit hun positie aan de top van de hiërarchische piramide van het Nederlandse openbaar bestuur, vaak ver afstaan van de systemen en applicaties die zij bespreken en beoordelen. Hoofdlijnen domineren, terwijl bij veel technologische toepassingen geldt dat *the devil in the detail* schuilt. Daarbij blijken sommige trajecten meerdere kabinetten en daarmee parlementaire samenstellingen te overbruggen, terwijl tegelijkertijd de ambities met het project verschuiven en veranderen. Zo discussieerde het parlement vele jaren over de toepassing van biometrie op het paspoort en:

"door de jaren heen is er veel begripsverwarring ontstaan, waar niemand echt zijn vinger achter kon krijgen. Steeds groter werden de termen en ambities als het ging over het doel dat de biometrie moest dienen: van 'look alike fraude' tot terrorismebestrijding; van verificatie van het paspoort tot identificatie bij rampen; van het beveiligen van het paspoort tot identiteitsfraude in brede zin. Maar de consequenties van deze grote termen voor de uitvoering worden niet consequent uitgewerkt" (Snijder 2010: 85).

Ook om andere redenen is een goede parlementaire controle lastig. Zo merkte Tweede Kamerlid Pieter Omtzigt (CDA) op dat het voor de Tweede Kamer niet altijd makkelijk is de voortgang van de invoering te volgen.

"Bij grote ICT-projecten is het lastig om een vinger aan de pols te houden. Bovendien is het lastig zicht te krijgen op de voortgang. Natuurlijk krijgen Kamerleden overzichtslijstjes van het aantal aangesloten zorgverleners en andere kengetallen, maar de planning en schema's blijken vaak te optimistisch" (Pluut 2010: 42).

De observatie van Omtzigt bevestigt de eerdere conclusies van de Algemene Rekenkamer over de gebrekkige informatievoorziening van ministers naar de Tweede Kamer, waardoor het onvoldoende mogelijk is de ICT-projecten voor aanvang te toetsen, de voortgang ervan te monitoren en de projecten te evalueren (Algemene Rekenkamer 2007a).

3.1.6 TERUGKOPPELING VAN ARGUMENTATIES

De ontwikkelingen tonen dat de typische argumenten die worden ingezet om een nieuw informatiesysteem te bepleiten, weinig aan kritiek worden blootgesteld. Weliswaar bestaat er in ambtelijke en politieke kringen op een individueel niveau zeker ook scepsis over ICT-oplossingen, mede als gevolg van allerlei mislukte projecten en informatievervuiling, in het bredere debat zorgen motieven als veiligheid, effectiviteit en efficiëntie, gecombineerd met het probleemoplossende 'imago' van ICT, als het ware voor zichzelf. In de dagelijkse politiek blijken het zwaarwegende argumenten, die veelal impliciet voorgaan op andere waarden als transparantie, privacy en steeds vaker ook keuzevrijheid. Zo laat Groothuis (2010) zien dat de afgelopen jaren in diverse wetten zodanige wijzigingen zijn aangebracht dat de overheid het internet als het verplichte communicatiekanaal kan opleggen. Het al vroeg in de ontwikkeling van de eOverheid verankerde uitgangspunt van keuzevrijheid voor de burger tussen papieren en digitaal verkeer met de overheid (Tweede Kamer 1997-1998) wordt meer en meer losgelaten. Tegelijkertijd benutten sommige overheidsorganisaties wel ten volle hun eigen keuzevrijheid als papieren verkeer hen beter uitkomt (Groothuis 2010: 351-352).[10] Ook de totstandkoming van de anonieme OV-chipkaart toont dat weinig op keuzevrijheid wordt voorgesorteerd. De mogelijk-heid van anoniem reizen werd pas onder druk van het CBP in de plannen opgenomen (Van 't Hof et al. 2010b), en toen deze mogelijkheid eenmaal werd geaccepteerd ontstond een anonieme chipkaart die een weinig aantrekkelijk alternatief biedt.

Hiernaast lijkt er in de politiek-bestuurlijke praktijk vaak sprake van een polarisatie tussen perspectieven die vertrekken vanuit de stuwende respectievelijk de verankerende beginselen. Alhoewel voormalig minister van Binnenlandse Zaken Ter Horst zich bij de aanbieding van het rapport van de Commissie Veiligheid en persoonlijke levenssfeer (januari 2009) uitsprak voor een zorgvuldige balans tussen de belangen van veiligheid en privacy en opmerkte dat de daadkracht op het terrein van veiligheid niet mag leiden "tot het te grabbel gooien van persoonsgegevens", stelde ze later dat jaar na de mislukte aanslag met de 'onderbroekbom' in december 2009 dat zij van de school van 'veiligheid boven privacy' is.[11] Deze polarisatie tussen belangen lijkt kenmerkend voor de wijze waarop veel beleidsmatige discussies rondom de inzet van ICT de afgelopen jaren zijn gevoerd. In het eerder aangehaalde Algemeen

Overleg uit 2001 over de noodzaak tot opname van een biometrisch kenmerk in reisdocumenten klinkt het reeds door in de opmerkingen van destijds nog Kamerlid Balkenende.

"De heer Balkenende hoopt dat bij deze noodzakelijke technische verbetering, de privacy geen belemmering zal gaan vormen. (…) De heer Balkenende verzoekt de minister te bevestigen dat bij artikel 3 van de Paspoortwet het privacyaspect niet aan de orde is, maar dat het gaat om een technisch kenmerk dat in de wet moet worden opgenomen" (geciteerd in Böhre 2010: 22).

Niet alleen veiligheid, maar ook de stuwende beginselen van effectiviteit en efficiëntie dragen op het politieke en beleidsniveau zorg voor de impuls van de ontwikkeling, introductie en operatie van steeds weer nieuwe en innovatieve ICT-systemen. Met name in de verdere uitbouw van de eOverheid worden deze motieven sterk aangezet.

Echte verantwoording van de claims die over veiligheid, effectiviteit en efficiëntie worden gemaakt, ontbreken echter vaak (Kearns 2004). Zo concludeerde een onderzoek naar digitalisering van de besluitvormingsprocessen in de bestemmingsplanketen: "Goed gefundeerd inzicht in te verwachten kosten en baten van digitalisering binnen de keten valt niet of nauwelijks te geven" (CapGemini en Ernst&Young 2004: 8). Diverse instanties hebben de afgelopen jaren meermalen aangegeven dat het veronderstelde causale verband tussen instrumenten en effecten in het veiligheidsbeleid niet of onvoldoende onderbouwd wordt (Van der Knaap 2010: 13). De Commissie evaluatie antiterrorismebeleid (commissie-Suyver 2009) wees in haar rapport van mei 2009 op de noodzaak van een integrale evaluatie van antiterrorismemaatregelen. In een reactie kondigde het kabinet een evaluatieonderzoek aan, waarvan de uitkomsten nog moeten worden afgewacht (Tweede Kamer 2008-2009d). ICT-evaluatie is al jaren een complex vraagstuk (Thaens 1998; Van Hout 2005). Wat bij het beoordelen van ICT-applicaties opvalt, is dat veelal niet wordt getoetst aan de beleidsrealiteit maar aan de termen van het systeem zelf, bijvoorbeeld in de vorm van de hoeveelheid hits die de Verwijsindex Risicojongeren genereert. Het motief zelf, maatschappelijke veiligheid, wordt nauwelijks van serieus 'bewijs' voorzien (vgl. Waldron 2007; Robinson et al. 2010: 7). Illustratief voor de gebrekkige motivatie is de gang van zaken rondom het EPD. De minister van VWS merkte in de memorie van antwoord aan de Eerste Kamer op: "De toegevoegde waarde van het EPD moet (...) worden gezocht in het gemak en de snelheid waarmee gegevens betrouwbaar en veilig kunnen worden uitgewisseld" (Eerste Kamer 2009-2010c: 6). Veel concreter dan bovenstaande algemene doelstellingen wordt het volgens Pluut (2010) in de eerste beleidsdocumenten niet.

"Beleidsmakers of ministers verwijzen niet naar onderzoeken die laten zien dat (landelijke) gegevensuitwisseling inderdaad leidt tot deze resultaten en leggen niet uit hoe, en onder welke voorwaarden, een l-EPD (landelijk EPD) tot verbeteringen in de zorg leidt. Daar is kennelijk geen reden toe: in de beginjaren lijkt er een soort algemene consensus over te bestaan dat er moet worden gewerkt aan landelijke informatievoorziening in de zorg" (Pluut 2010: 23).

Pas later, naarmate de planvorming en implementatie vorderden en het parlement zich toenemend kritisch toonde, kwamen in de officiële documenten meer verwijzingen voor naar onderzoeksrapporten die de noodzaak van een EPD zouden aantonen. In deze onderbouwing verschoof de doelstelling in de loop van de tijd echter van financiële overwegingen (efficiëntie) naar (medicatie) veiligheid.

Box 3.1 Magie met getallen: 19.000 vermijdbare fouten

In hun pleidooi voor een landelijk Elektronisch Patiëntendossier (EPD) verwijzen opeenvolgende ministers naar het *HARM rapport* (Van den Bemt 2006), een wetenschappelijk onderzoek dat concludeert dat van de gemiddeld 41.000 geneesmiddel-gerelateerde ziekenhuisopnames per jaar er 19.000 potentieel vermijdbaar zijn. De belangrijkste aanbeveling van het rapport is patiënten die (aanleg voor) één of meerdere risicofactoren vertonen, proactief te benaderen voor extra medicatiebegeleiding. Betere informatie-uitwisseling is volgens de onderzoekers een van de instrumenten om deze betere begeleiding te realiseren, zonder dat daarbij elektronische patiëntendossiers expliciet aan de orde komen.

In reactie op vragen uit de oppositie licht minister Klink bij de plenaire behandeling van het wetsvoorstel nogmaals toe: "De gegevens over 19.000 mensen die in een ziekenhuis worden opgenomen en de 1200 van hen die overlijden, zijn afkomstig uit het HARM-onderzoek van 2006. Het komt er op neer dat per dag 60 mensen worden opgenomen wegens medicatiefouten, van wie er een drietal per dag overlijdt." Mevrouw Gerkens (SP) reageert op minister Klink met de vraag: "(...) of de minister een inschatting heeft gemaakt hoeveel medische missers door het EPD voorkomen gaan worden, anders gezegd hoeveel patiëntverbetering kan worden verwacht en hoeveel kans er is op missers door het EPD. (...)."

Minister Klink antwoordt: "Die inschatting is wel degelijk gemaakt. Ik noemde niet voor niets die 19.000 ziekenhuisopnames vanwege medicatiefouten. Een groot deel – ik kan echt niet zeggen hoe groot – daarvan kan worden ondervangen door een verbetering in het inzicht in de medicatie. (...) Ik vind percentages helemaal niet zo relevant. Al kunnen er maar een paar gevallen per dag op de spoedeisende hulp beter worden geholpen, dan is het al goed" (Tweede Kamer 2008-2009a: 3936-3937). Mevrouw Agema (PVV) mengt zich ook in de discussie en stelt: "In het HARM-onderzoek wordt nergens gerept van een meerwaarde van het Elektronisch Patiëntendossier bij verlaging van het aantal vermijdbare ziekenhuisopnamen. (...) Mijn punt is dat het EPD mogelijk – hoe veel

weten wij niet, want dat antwoord kon ook mevrouw Gerkens niet worden gegeven – kan zorgen voor minder vermijdbare fouten, maar ook meer vermijdbare fouten. In het EPD kunnen immers ook fouten staan. (…) De minister gebruikt een argument: het EPD moet, omdat het voor minder vermijdbare fouten zorgt, maar – als ik nu even de wetenschapper Klink mag aanspreken – die redenering kan ook de andere kant op gaan. Wij hebben geen bewijs.” Minister Klink pareert de uiteenzetting van mevrouw Agema als volgt: “Neemt u dan maar een keer op gezag van de wetenschapper Klink aan dat het toch werkt en dat het toch tot minder fouten zal leiden” (Tweede Kamer 2008-2009b: 3946-3947).

Inmiddels maakt het kabinet naar aanleiding van de rapportage *Sociale Veiligheid ontsleuteld* (SCP 2008) meer werk van doelstellingen en indicatoren waarop het veiligheidsbeleid kan worden beoordeeld. Beleidstheoretisch onderbouwd rapporteren wint aan populariteit, maar het vizier van dit type rapporteren richt zich slechts spaarzaam op de onderbouwing van verwachtingen en latere beoordeling van de maatregelen van ICT-initiatieven. Soms wordt expliciet gesteld dat het ‘succes’ van een applicatie zich aan meetbaarheid onttrekt, zoals gebeurde met betrekking tot de vraag of cameratoezicht voor meer veiligheid zorgt.[12] Deels weet men soms ook niet wat precies gemeten dient te worden of in welke grootheden dat moet worden uitgedrukt. Het *Eindrapport Evaluatie cameratoezicht op openbare plaatsen* uit eind 2009 concludeert dat geen eenduidig beeld is te geven van de effecten van cameratoezicht op de veiligheid (Tweede Kamer 2009-2010a).[13] Bovendien zijn de kosten van de projecten wel, maar de baten niet goed in kaart te brengen. Maar ook aan de kostenkant is te zien dat waar er ramingen zijn, er dikwijls te rooskleurig is gedacht over de duurzaamheid van technologie. Zo wordt een digitaliseringsoperatie vaak ingeboekt als een eenmalige actie, maar wordt er geen rekening gehouden met kosten op lange termijn voor zaken als onderhoud, beveiliging en updates van het systeem (Keymolen & Prins 2011). De ambitie de effecten van de inzet van ICT-toepassingen te meten levert soms ook paradoxale consequenties op, zoals bleek uit de reactie van de Britse politie toen de UK House of Commons Home Affairs Committee de Britse regering opriep te onderzoeken of diverse maatregelen, waaronder cameratoezicht, inderdaad tot een daling van de criminaliteit leiden (House of Commons 2008). De politie liet daarop in een reactie weten dat er dan echter eerst een nationale databank van camerabeelden moest komen.[14]

3.1.7 STUWENDE, VERANKERENDE EN PROCESMATIGE BEGINSELEN

Hoe worden de stuwende, verankerende en procesmatige beginselen ingezet in en gevormd door de geschetste politiek-bestuurlijke praktijk op rijksniveau? Allereerst blijkt dat de betekenis die aan deze beginselen wordt gegeven verre van eenduidig is. Tevens laat het voorgaande zien dat de weging van stuwende, veran-

kerende en procesmatige beginselen niet wordt bepaald door een strakke choreografie. Twee tendensen lijken van invloed op de onvaste manier waarmee in de praktijk met deze beginselen wordt omgesprongen. In de eerste plaats bestaat de neiging om instrumenteel over ICT te denken. In het verlengde daarvan ontbreekt een besef van de veranderingen die ICT voor de aard en het functioneren van de overheid teweegbrengt.

Het voorgaande laat zien dat veel bestuurlijke 'eigenaren' of pleitbezorgers van ICT-applicaties de neiging hebben om ICT als een instrument – een voertuig – te zien. Er zijn veel ambities *met* informatietechnologie, en veel minder *voor* informatietechnologie. De belofte van de technologie is – in ieder geval in de ogen van veel bestuurders – om het bestaande beter te doen. Niet anders, maar beter. Dit is op veel plaatsen terug te zien: van het sleutelen aan de dienstverleningskwaliteit van de overheid tot het beter aanpakken van zorgtaken van de overheid, zoals medicatieveiligheid in het EPD. In bestuurlijke termen is de aanname – die ook regelmatig wordt uitgesproken – dat het primaire proces niet verandert. Een belangrijk gevolg van dit uitgangspunt is dat de onbedoelde doorwerking die digitalisering wel degelijk – alleen al omdat burgers veranderd zijn – op het functioneren van de overheid (het 'primaire proces') heeft, niet of nauwelijks wordt onderkend of waargenomen. Hoewel de instrumentele dimensie van ICT belangrijk is, leidt deze houding tot een evaluatieve armoede, die zich toont in het feit dat geloofwaardige evaluaties van applicaties zeldzaam zijn. Bovendien ontstaat een tekort aan maatstaven voor de beoordeling van applicaties wanneer die alleen maar instrumenteel worden afgerekend. Dan blijven discussies steken in de veiligheid van de technologie (OV-chipkaart) of in financiële debacles (zoals de diverse mislukte ICT-projecten). Met andere woorden: de blik vernauwt zich tot de vraag of de technologie haar belofte waarmaakt, namelijk om het bestaande beter (effectiever en efficiënter) te doen. Waar gesproken wordt in termen van kosten blijft de discussie dikwijls beperkt tot personele of financiële implicaties. De bredere implicaties blijven buiten beeld, waardoor zij niet in de afweging betrokken worden – of die nu vooraf plaatsvindt (besluitvorming) of achteraf (evaluatie). Illustratief zijn de passages over kosten/baten in het projectvoorstel dat de Immigratie- en Naturalisatiedienst (IND) indiende onder het kabinetsprogramma 'ICT-projecten in maatschappelijke domeinen'. Het voorstel betrof de ontwikkeling van een systeem (genaamd No-Q) voor de geautomatiseerde grenspassage van ongeveer drie miljoen vertrekkende EU-passagiers op Schiphol. De kosten en baten werden geconcretiseerd in enerzijds (kosten) de benodigde personele en financiële investeringen en anderzijds (baten) een "meetbare reductie van wachtrijen en wachttijden", efficiëntieverbetering bij de verificatie van reisdocumentenpercentages ("ombuigen van de kostentoename") en het "maximaliseren van de veiligheid". Zowel de kosten als de baten werden uitsluitend instrumenteel afgerekend.[15]

Zo blijft ook buiten beeld dat ICT soms een fundamentele verandering van de taakopvattingen van de overheid bewerkstelligt. De gedachte heerst nog steeds dat informatietechnologie intrinsiek betekenisloos is, aldus een naaste medewerker van Eurocommissaris Kroes voor de Digitale Agenda.[16] Maar deze techniek is niet, of niet alleen, een voertuig van verandering, het is ook zelf een verandering. Zelfs daar waar digitalisering de meest neutraal ogende vooruitgang heeft geboekt, namelijk in de rationalisering van de interne werkprocessen ('bedrijfsvoering') van de overheid, is die zelfstandige betekenis aan te wijzen. Ook daar is te zien dat ambities *met* ICT niet gepaard gaan met ambities *voor* ICT. Een ambitie voor ICT zou in deze context bijvoorbeeld zijn om een nieuwe applicatie daadwerkelijk te integreren met de organisatie, met de mensen en hun verwachtingen. In plaats hiervan is er in de praktijk vaak sprake van gescheiden werelden van techniek en organisatie, waarbij men gaandeweg moet constateren dat systemen niet aansluiten op de werkvloer (zoals najaar 2010 nog met het politiesysteem Basisvoorziening Handhaving – BHV) en dat beoogde gebruikers een nieuw systeem soms zelfs om allerlei redenen ondergraven of ontduiken. Achter het zogenaamde primaire proces blijkt een rijk scala aan werkprocessen en waardenoriëntaties schuil te gaan (Van den Akker & Kuiper 2008: 161). Door de interactie tussen de techniek en de mensen die ermee werken verandert het functioneren van de overheid, soms op een onvoorziene manier. Diverse voorbeelden laten zien dat technologische mogelijkheden de doelen van de overheid sterk beïnvloeden. Huidige en populaire (beleids)doelen als 'maatwerk' en proactief beleid zijn ondenkbaar (of niet te realiseren) zonder deze achtergrond van digitalisering. ICT wordt desondanks neutraal gekenschetst, waardoor buiten beeld blijft dat nastrevenswaardige zaken als maatwerk – zelfs in de context van dienstverlening – of proactief beleid wel degelijk ook de overheid zelf veranderen. Deze doelen veronderstellen namelijk dat de overheid dichter op de huid van de burger komt, met alle meer en minder wenselijke consequenties van dien. Maar achter de beslissingen die deze veranderingen in gang zetten, ontbreken in de praktijk de brede afwegingen, waarin ook de verankerende en procesmatige beginselen een volwaardige plaats krijgen. De meningen in *civil society* over bijvoorbeeld het EPD zijn zoals eerder werd opgemerkt sterk verdeeld. Maar er is op beleidsniveau geen forum waarin deze veelzijdigheid tot uitdrukking kan komen.

3.2 CONCLUSIE

ICT is met veel enthousiasme door politiek en bestuur omarmd en heeft een zichtbare invloed op diverse beleidsterreinen. Door de overheersende neiging om instrumenteel over ICT te denken en debatteren is veel minder zichtbaar dat ICT tegelijkertijd op fundamentele wijze de aard, taakopvatting en het functioneren van de overheid verandert. De discussie daarover en over de consequenties die dat heeft voor de relatie tussen overheid en burger(s) wordt niet of nauwelijks gevoerd.

Vanuit de stuwende, verankerende en procesmatige beginselen bezien valt de discussie over de consequenties op het vlak van de stuwende beginselen nogal eens ten prooi aan een retorische vorm van verantwoording (Robinson et al. 2010). Meer effectiviteit en meer veiligheid behoeven in het debat vaak weinig betoog. Bij het denken over de consequenties voor de verankerende beginselen ontbreekt vaak een diepgravende analyse. In de praktijk wordt ze veelal gereduceerd tot een privacyparagraaf in de memorie van toelichting. Ook wordt de feitelijke tendens naar dwingende informatisering van de relatie overheid-burger en naar afnemende keuzevrijheid voor lief genomen, terwijl het in theorie nog steeds heet dat 'onwillige' burgers moeten kunnen kiezen voor het 'papieren kanaal'. Dat bijvoorbeeld een persoon anoniem met een OV-chipkaart moet kunnen reizen stond niet in de oorspronkelijke voorstellen, en is ook nadien slechts minimaal vormgegeven. Op het vlak van de procesmatige beginselen is weinig aandacht voor het doordenken van consequenties van digitalisering en evenmin om het inrichten van adequate arrangementen voor als het fout gaat. Mogelijk dat de afweging van beginselen onder het kabinet-Rutte explicieter op de agenda zal staan nu in het regeerakkoord is afgesproken dat "De informatie-veiligheid en bescherming van persoonsgegevens worden verbeterd. Voorgenomen maatregelen inzake opslag, koppeling en verwerking van persoonsgegevens worden zoveel mogelijk voorzien van een horizonbepaling en bij de voorbereiding nadrukkelijk getoetst aan effectiviteit" (Regeerakkoord 2010: 42).

Een meer omvattende benadering die besloten ligt in een reële afweging van stuwende, verankerende en procesmatige beginselen kan alleen worden opgepakt wanneer ICT gepolitiseerd wordt. Dit politiseren komt, zoals uit het voorgaande duidelijk werd, langzaam steeds meer in beeld: door de Eerste en Tweede Kamer, maar ook door burgerbewegingen. Wel vertoont dit nog een grillig beeld: het is weinig voorspelbaar op welke onderwerpen (applicaties) wel en op welke niet wordt aangeslagen. In gevallen waarin een voorgestelde applicatie overduidelijk neerkomt op een ingreep in de maatschappelijke verhoudingen is in ieder geval duidelijk dat de invoering door middel van het zwaarst mogelijke instrument zal plaatsvinden, namelijk de parlementaire wet. Maar ook dan kan de discussie door een overdreven vertrouwen in (het instrument) ICT geneutraliseerd worden, zoals het voorbeeld van de databank met biometrische kenmerken in eerste instantie heeft laten zien. In andere gevallen heeft de voorgestelde applicatie meer weg van een neutraal technisch 'dingetje', en dan zal de neiging groot zijn om er zo min mogelijk discussie over te entameren. Maar ook in een ogenschijnlijk 'dingetje' als het BSN schuilen klemmende maatschappelijke vraagstukken. Het blijft zaak om de bredere consequenties zo goed mogelijk te inventariseren en te wegen.

De belangrijkste conclusie is echter dat, terwijl over technologie en applicaties ondanks een zekere instrumentele inslag soms al wel stevige discussies gevoerd worden, dit voor informatiestromen en koppelingen tussen applicaties nagenoeg

niet het geval is. De vele voorbeelden laten zien dat de uitdaging om aan informatiestromen en koppelingen een zelfstandige betekenis toe te kennen, en die betekenis ook politiek te onderkennen, niet of nauwelijks wordt opgepakt. Het verantwoordingsmoment is ten aanzien van deze kwesties vaak nog summierder dan bij applicaties. 'We koppelen bestand X en Y, omdat ons dat het potentiële voordeel Z oplevert' is vaak de meest uitgewerkte variant van verantwoording die kan worden aangetroffen. Ook hier vernauwt de vraagstelling zich tot de wenselijkheid van de doelstelling (Z). De ICT wordt slechts afgerekend op de vraag of het die doelstelling succesvol naderbij brengt. Verantwoording over informatiestromen blijkt nog niet op het netvlies van politiek en beleid te staan.

NOTEN

1 Zie uitgebreid: Böhre 2010.

2 Zie onder meer de pilot 'No-Q' die op 26 mei 2010 op Schiphol van start ging http://www.rijksoverheid.nl/nieuws/2010/05/26/elektronische-grenspassage-van-start.html.

3 NUP (2008) Nationaal Uitvoeringsprogramma Dienstverlening en eOverheid. 'Burger en Bedrijf Centraal', behorende bij verklaring d.d. 1 december 2008 vastgesteld bij gelegenheid van het Bestuurlijk Overleg van rijk, provincies, gemeenten en waterschappen over de realisatie van het Nationaal Uitvoeringsprogramma Dienstverlening en e-overheid, blz. 3.

4 Zie voor een overzicht Tweede Kamer 2009-2010k.

5 Interviews met dhr. M. Hillenaar, Rijks-CIO, ministerie van BZK, november 2009 en maart 2009.

6 Het Expertise Centrum, brief inhoudende Toetsing kosten-batenanalyse No-Q, Den Haag, 15 december 2008.

7 Zie voor een zeer kritische beoordeling van dit voorstel: Raad van State 2010: 141-142.

8 Gesprek met de Eerste Kamerleden R.H. van de Beeten, H. Franken, J. Hamel, P.L. Meurs, I.Y. Tan, C.P. Thissen; mei 2010. Leden van de Raad van State gaven een soortgelijk signaal, april 2010 (gesprek met C.J.M. Schuyt, M. Oosting, M. Raijmakers, H.J.Th.M. van Roosmalen, Raad van State). De Raad had in het wetgevingstraject over biometrie op het paspoort een advies-conform uitgebracht.

9 Gesprek met de Eerste Kamerleden R.H. van de Beeten, H. Franken, J. Hamel, P.L. Meurs, I.Y. Tan, C.P. Thissen, mei 2010.

10 Zo geeft de jurisprudentie over art. 2:15 Awb diverse voorbeelden van situaties waarin communicatie via het digitale kanaal een overheidsinstantie (achteraf) niet van pas kwam en de instantie zich op het formele standpunt stelde dat het digitale kanaal niet was opengesteld (Groothuis 2010).

11 Minister Ter Horst deed deze uitspraak op 30 december 2009 tijdens een persconferentie naar aanleiding van de mislukte aanslag op een vlucht van Schiphol naar Detroit op 25 december 2009.

12 Overigens heeft Regioplan inmiddels het Beslisinstrument Continueren Cameratoezicht (BICC) ontwikkeld, waarmee gemeenten een kapstok wordt geboden voor evaluatieonderzoek en ze een gefundeerd besluit kunnen nemen of ze met cameratoezicht willen stoppen of doorgaan. *Secondant* 3-4 2010: 58-61.

13 Deze conclusie werd in het Verenigd Koninkrijk eveneens getrokken in een onderzoek van de Liberal Democrats: http://www.thisislondon.co.uk/news/article-23412867-tens-of-thousands-of-cctv-cameras-yet-80-of-crime-unsolved.do.

14 http://tweakers.net/nieuws/53877/brits-parlement-vreest-privacyrisicos-id-database.html.

15 Immigratie- en Naturalisatiedienst (IND), Aanvraag investeringsimpuls ICT in maatschappelijk domein, Projectplan No-Q, 15 december 2008.

16 Gesprek met de heer C. van Oranje, kabinet van Eurocommissaris Kroes, Brussel, maart 2010.

4 VAN BELEID NAAR eREALITEIT

De ambities voor nieuwe systemen en de roep om meer en rijkere informatie ontstaan niet alleen in Den Haag. Naast de plannen van de nationale overheid die in de Eerste en Tweede Kamer worden besproken werkt een variëteit aan uitvoerende en lokale partijen, relatief autonoom en relatief ver weg van de parlementaire controle, aan eigen plannen en initiatieven. Niet alleen vindt de 'uitrol' van de elektronische overheid dicht bij de uitvoeringspraktijk plaats, zij wordt daar ook in belangrijke mate gevormd. Er is veel ruimte voor initiatieven van onderaf. Landelijke systemen, waarover in het parlement gedebatteerd wordt, zijn ook vaak niet meer dan paraplu's die boven een veelheid van reeds bestaande lokale initiatieven worden gehangen. Dit is bijvoorbeeld het geval bij het EPD en bij de Verwijsindex Risicojongeren. Voordat een systeem officieel wordt gelanceerd – door het rijk, uitvoeringsorganisaties of lokaal – is er bovendien vaak al uitgebreid ervaring mee opgedaan, ofwel in erkende *pilots* ofwel doordat een applicatie feitelijk al in gebruik is genomen, ongeacht formele besluitvorming. Illustratief voor het laatste is ANPR, de automatische kentekenherkenning (zie par. 4.3).
Er is dus alle reden om te kijken naar de gebruikerskant van de applicaties van de eOverheid, zeker in die gevallen waar gebruiker en ontwikkelaar dezelfde zijn. Hier treft men spelers aan als de Belastingdienst en andere grote uitvoeringsinstanties, die al jaren vooroplopen als het om de kansen van digitalisering gaat. Ook gemeenten laten zich zien: vanuit de lokale behoeften ontwikkelden zij bijvoorbeeld een eigen nadere visie op het Elektronisch Kinddossier. Politiekorpsen breiden het arsenaal van informatie-instrumenten gestaag uit, het Bureau Keteninformatisering Werk en Inkomen (BKWI) is uitgegroeid tot een cruciale gegevensleverancier voor alle zogeheten Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI)-organisaties, die op hun beurt weer samenwerken in het digitaal klantdossier (DKD). De Belastingdienst biedt burgers de mogelijkheid via een beveiligde portal online aangifte te doen en de SVB werkt aan de uitbouw van de zogenaamde Burgerpolis (www.burgerpolis.nl), waar burgers niet alleen een persoonsgebonden overzicht van hun sociale zekerheidssituatie kunnen opvragen, maar ook ervaringen over sociale zekerheid met elkaar uitwisselen.

4.1 GRENZELOZE UITVOERING

4.1.1 EEN VEELHEID VAN SPELERS EN MOTIEVEN

De Rijksdienst voor het Wegverkeer (RDW) heeft de afgelopen jaren hard gewerkt aan de *business case* voor het zogenaamde eRijbewijs. "Concluderend is er de kans om een chip op het rijbewijs te plaatsen om zowel verbeterde fraudebestrijding als e-dienstverlening vorm te geven" (RDW 2008: 5). De RDW wil de mogelijkheid die de derde richtlijn Europese rijbewijzen[1] biedt om een chip op het rijbewijs te

plaatsen voor meer gebruiken dan alleen om aan de nieuwe Europese eisen voor fraudegevoeligheid van het rijbewijs te voldoen. De dienst ziet ook kansen een belangrijke eOverheid-speler te worden: laat het rijbewijs uitgroeien tot een breed toe te passen identificatie-instrument dat een hoog niveau van elektronische authenticatie[2] biedt voor allerhande digitale diensten van de overheid. De ambitie van de RDW heeft alles te maken met het ontbreken van een goede overheidsvoorziening voor dit hoge niveau van authenticatie. Momenteel bieden alleen private partijen middelen voor een hoog niveau van authenticatie aan, maar nu patiënten de gegevens in hun EPD moeten kunnen inzien of zelfs aanpassen en burgers elektronisch hun kenteken gaan overschrijven blijken de waarborgen van het huidige DigiD (waar met password en sms-systeem wordt gewerkt) onvoldoende. Tenminste drie departementen zagen kansen hun toekomstige positionering binnen de eOverheid te versterken en startten eigen initiatieven. Naast het eRijbewijs van de RDW doet het ministerie van EZ via het programma eHerkenning een poging en zet het ministerie van BZK in op zowel een nieuwe versie van DigiD als een doorstart van de eerder gestrande elektronische Nederlandse Identiteitskaart (eNIK). Kenmerkend voor de initiatieven is dat de meerderheid van de partijen ervan uitgaat dat de inbreng van marktpartijen cruciaal is om het systeem succesvol te maken (CapGemini Consulting 2010a: 14). Samenwerken over de grenzen van de publieke sector heen lijkt een leidend motto. “De RDW overweegt de elektronische authenticatie ook voor private partijen beschikbaar te stellen” (RDW 2008: 15).

Aan de wens en noodzaak de grenzen van de eigen organisatie te overbruggen en met andere instanties samen te werken bij het benutten van applicaties (ID-kaart) en informatie, ligt op uitvoeringsniveau een variëteit aan motieven ten grondslag. Voor de RDW liggen die, behalve in fraudebestrijding en efficiëntere dienstverlening, in de eigen toekomstige positionering binnen de eOverheid. Andere samenwerkingsarrangementen zijn volgens de initiatiefnemers ingegeven vanuit ‘de pure noodzaak’ om in gezamenlijkheid complexe maatschappelijke problemen aan te pakken, zoals de Verwijsindex Risicojongeren bij sociale veiligheid illustreert (Keymolen & Prins 2011; Holvast & Bonthuis 2010). Weer andere samenwerking is geïnitieerd omdat ingewikkelde beleidsinitiatieven waar meerdere organisaties bij betrokken zijn (uitkeringen, zorgtoeslagen) anders onmogelijk tot een goed einde te brengen zijn. Soms verenigen de uitvoerende instanties zich meer expliciet, zoals de Manifestgroep, een initiatief van elf uitvoeringsinstellingen[3] van de overheid, die burgers en bedrijven overheidsbrede informatie en diensten aanbieden. Meer algemeen, ten slotte, zijn diverse van de initiatieven het gevolg van tekortschietend beleid op departementaal niveau rondom de eOverheid (Gateway NUP 2009).[4]

Wie kijkt naar de wijze waarop de inzet van ICT in de uitvoeringspraktijk heeft vorm gekregen ziet kortom een rijkgeschakeerd landschap van motieven en samenwerkingsvormen, een variëteit aan mechanismen voor de uitwisseling van

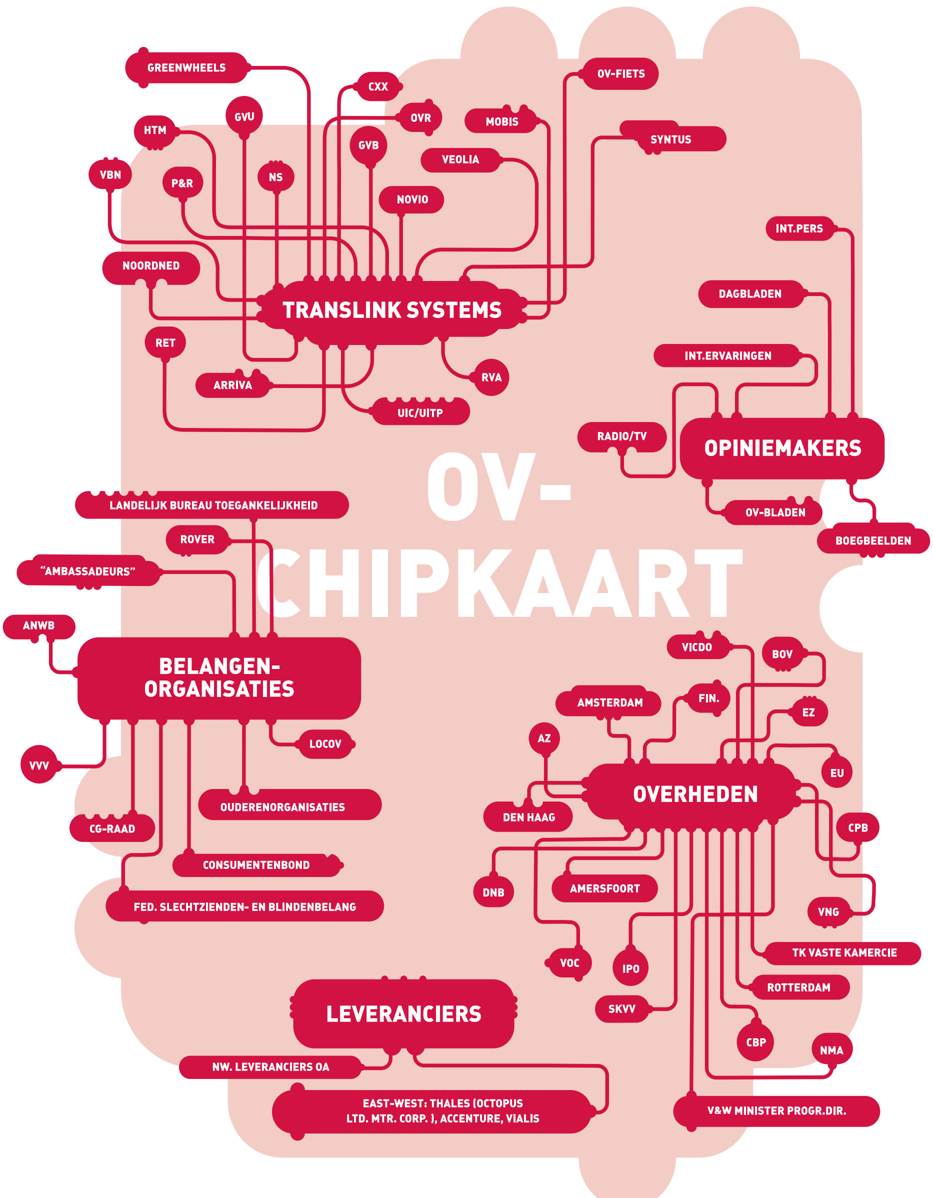
informatie en een bont en diffuus gezelschap van betrokken partijen. Als er al iets zou zijn als *de* eOverheid, op uitvoeringsniveau bestaat die in ieder geval niet. Bovendien gaat het op uitvoeringsniveau lang niet altijd om organisaties met een uitgekristalliseerde structuur en een rationele ordening van mensen en middelen. "Een kenmerk van virtuele organisaties is juist het ontbreken van een heldere structuur en duidelijke organisatiegrenzen. Virtuele organisaties worden vaak gekenmerkt door beweging, door steeds wisselende processen van elektronische in- en uitsluiting" (Bekkers 2000: 12). Illustratief is hier RINIS, het Routerings Instituut voor Informatiestromen in de Sociale Zekerheid, dat fungeert als een informatiemakelaar die bemiddelt tussen vraag en aanbod van informatie. In oorsprong waren het de Sociale Verzekeringsbank, het Landelijk Bureau Inning Sociale Verzekeringen en het Landelijk Instituut Sociale Verzekeringen die met de oprichting van RINIS de stap zetten op het pad van intersectorale gegevensuitwisseling (Kinkhorst 2000: 182; Bekkers & Thaens 2005: 143). Inmiddels bedient RINIS elf 'sectoren'[5] en werden in 2009 ruim 117 miljoen berichten uitgewisseld (RINIS 2010: 3), wat bijna een verdubbeling is ten opzichte van 2008. De uitwisseling gaat ook over de grenzen heen: de SVB en het College voor Zorgverzekeringen (CVZ) ontvangen en versturen via RINIS berichten aan en van Europese zusterorganisaties (RINIS 2010). Bekkers spreekt in dit verband over kolonisatie en grensvervaging: "Steeds meer domeinen, buiten de sociale zekerheid, worden door het RINIS ontsloten. Het domein van RINIS breidt zich steeds verder uit, waardoor de grenzen tussen allerlei domeinen beginnen af te brokkelen" (Bekkers 1998: 139-140).

4.1.2 BELEIDSDOMEINEN, DIENSTEN EN MOTIEVEN INTERFEREREN

Waar Bekkers destijds de eerste tekenen van een afbrokkeling zag, lijkt de afbouw van de grenzen nu, tien jaar later, in virtuele zin steeds meer een realiteit. Vaak dient een en dezelfde applicatie of informatiebron tegelijkertijd dienstverlening, controle en zorg. Steeds vaker ook, worden dezelfde gegevens in verschillende applicaties gebruikt. De illustraties liggen inmiddels voor het oprapen en wie het meldingenregister van het College Bescherming Persoonsgegevens erop naspeurt, ontwaart vele verrassende samenwerkingsarrangementen. Organisaties als het UWV, Centrum voor Werk en Inkomen (CWI) en SVB delen al jaren als 'ketenpartners' – eigenlijk zijn het netwerkpartners – in het domein van werk en inkomen hun gegevens met behulp van het Bureau Keteninformatisering Werk en Inkomen (BKWI). Maar enkele jaren geleden zijn ook diensten uit het opsporingsdomein zoals de Arbeidsinspectie en Sociale Inlichtingen- en Opsporingsdienst (SIOD) aangeschoven. Het College Bescherming Persoonsgegevens deed in 2010 onderzoek naar de praktijk van deze laatste organisatie om op basis van gegevens die ze verkrijgt van gemeenteambtenaren, de Belastingdienst en het Openbaar Ministerie risicoprofielen op te stellen die niet alleen worden gebruikt voor het opsporen van bijstandsfraude, maar ook worden benut om burgers op te sporen die een

risico hebben voor crimineel gedrag en overlast of die wat extra ondersteuning zouden kunnen gebruiken. Voor deze laatste toepassing worden dan weer gegevens van leerplichtambtenaren in de koppeling en profilering betrokken

Figuur 4.1 Betrokken bij het ontwikkelproces van de ov-chipkaart



Gebaseerd op het programma OV2Pay, opgenomen in ECP-EPN (2010: 23).

(CBP 2010b). Illustratief zijn ook de koppelingen die de Dienst Uitvoering Onderwijs (voorheen Informatie Beheer Groep) maakt. Gegevens worden, al dan niet geanonimiseerd, uitgewisseld met onder meer de GBA, de Dienst Sociale Zaken, de Belastingdienst, de Sociale Verzekeringsbank, Justitie, diverse onderwijsinstellingen en Adviesbureaus voor Opleiding en Beroep. "Daarnaast is het mogelijk dat de minister van Onderwijs, Cultuur en Wetenschap (OC&W) het Centraal Bureau voor de Statistiek of een onderzoeksbureau inhuurt om een nauw omschreven klantgroep te benaderen."[6]

Ook bij de OV-chipkaart is sprake van een complexe vervlechting, in dit geval van diensten, actoren en sectoren (zie figuur 4.1). Al toen de eerste plannen op de tekentafel lagen schoven er tientallen partijen aan, zo toont figuur 4.1: diverse overheden (het ministerie van Verkeer en Waterstaat (V&W) en 35 decentrale overheden met verantwoordelijkheden en bevoegdheden op het terrein van openbaar vervoer), een scala aan vervoersbedrijven, reizigersorganisaties, de Algemene Nederlandse Wielrijders Bond (ANWB) en allerhande derden, waaronder 'kaartuitgevers' als banken en Albert Heijn, en de providers die de communicatiesystemen en andere apparatuur leveren (De Kok et al. 2001: 298). De Belastingdienst heeft zich ontwikkeld tot een centraal schakelpunt voor controles aangaande fraude in de sociale zekerheid en in de zorg. In een gesprek met enkele leden van de Eerste Kamer werd opgemerkt dat koppelingen overigens selectief worden gelegd; wel als het gaat om de detectie van fraude en niet als het gaat om het uitbetalen van toeslagen.[7] Alhoewel de Belastingdienst al jaren bevoegdheden heeft om bij derden informatie op te vragen (Zwenne 1998), verzamelt de dienst vanuit de ambitie om "de administratieve rompslomp voor de burger niet te doen toenemen" grote hoeveelheden informatie buiten de belastingbetaler om.[8] Dit gebeurt niet alleen bij vertrouwde instanties als het Kadaster, de Kamers van Koophandel, werkgevers en banken, maar ook via websites als Marktplaats, LinkedIn en sociale netwerken.

Overigens is de samenwerking steeds vaker niet langer een kwestie van personen die besluiten om gegevens en dossiers uit te wisselen, maar interfereren de domeinen op een volautomatische wijze: wanneer het Centraal Justitieel Incassobureau (CJIB) besluit tot het innen van een niet-betaalde verkeersboete wordt de keuze formeel gemaakt door de officier van justitie. In materiële zin gebeurt dat volautomatisch door de computer. Vervolgens kan het CJIB "via de geautomatiseerde verwijsindex van het RINIS verhaal zonder dwangbevel halen op inkomsten uit arbeid en periodieke uitkeringen" (Bekkers 1998: 93). Dienstverlening en controle zijn twee kanten van de medaille, aldus twee leidende personen achter de introductie van de zogenaamde basisregistraties, Luitjens en Schravendeel.

> "Basisregistraties maken gegevensverkeer mogelijk. Die mogelijkheden kunnen door de overheid worden ingezet om de burger te controleren en in de touwen te houden, maar ook om hem beter van dienst te zijn (…), te betrekken in het democratisch proces en transparant te maken welke gegevens de overheid heeft en wat ze daarmee doet. Eerder noemden we dat twee kanten van dezelfde medaille" (Schravendeel & Luitjens 2001: 362).

4.1.3 DE GEREEDSCHAPSKIST VAN DE eUITVOERING

Natuurlijk is op uitvoeringsniveau de versmelting van informatieprocessen en de fluïde grens tussen beleidsdomeinen niet van recente datum. Diverse uitvoeringsorganisaties bieden andere partners in de publieke sector al jaren de mogelijkheid om hun systeem online te raadplegen en mutaties door te voeren (Bekkers 1998: 135). Ook in de wetenschappelijke literatuur was er in de jaren negentig al aandacht voor de invloed van informatisering op zowel de verhouding tussen beleidsontwikkeling en beleidsuitvoering als de traditionele grenzen tussen beleidssectoren op uitvoeringsniveau (Snellen 1994; Van de Donk & Frissen 1994). Daarbij is de nieuwe overheid meer dan eens in fraaie bewoordingen geduid: gekoppelde staat (Hirsch Ballin 1993), V*irtual fortress* (Taylor & Van Every 1993), infocratie (Zuurmond 1994) en virtuele staat (Frissen 1996). Sindsdien is met alleen maar meer enthousiasme gewerkt aan de verdere uitbouw van deze andere overheid. Recente beleidsinitiatieven als de stroomlijning van basisgegevens en populaire arrangementen als ketens (in de praktijk vaak netwerken) en verwijsindexen hebben de uitbouw van een digitaal verknoopt uitvoeringsniveau de laatste jaren in een stroomversnelling gebracht. Met het nieuwe gereedschap verandert ook langzaam de administratieve werkelijkheid van de overheid. Een werkelijkheid die vervolgens meer en meer het beeld van de overheid op de samenleving lijkt te gaan bepalen. De leidende initiatieven en arrangementen zijn als volgt samen te vatten en te karakteriseren:

– het werken in ketens en netwerken;
– het benutten van dezelfde gegevens binnen meerdere applicaties, meerdere organisaties en ten behoeve van meerdere e-dossiers;
– het realiseren van verwijsindexen[9], koppelvlakken[10] en landelijke schakelpunten[11] voor de noodzakelijke verbindingen en daarmee gegevensstromen in deze ketens en tussen deze dossiers en
– het stroomlijnen van dit gegevensverkeer met behulp van het Burgerservicenummer (BSN) en authentieke registraties zodat alle instanties één eenduidig en uniek persoonsnummer en gezaghebbende bronnen van informatie ter beschikking staat.

"In theorie is het dan altijd duidelijk waar de informatie kan worden gevonden en wie daarvoor de verantwoordelijkheid draagt. Ook is (in theorie) duidelijk voor

welke doelen de informatie bruikbaar is en kan op de gevonden informatie worden vertrouwd" (Algemene Rekenkamer 2010a: 18). De praktijk daarentegen blijkt weerbarstiger, zo laten de identiteitsfraudezaken van de heer Kowsoleea en diverse andere burgers zien (Buruma 2011; Nationale Ombudsman 2009a). Illustratief voor de weerbarstigheid is ook de opstelling van de Belastingdienst bij het gebruik van de GBA. Omdat de kwaliteit van de GBA niet volledig is gegarandeerd, heeft de Belastingdienst bij het ministerie van BZK ruimte bedongen van de basisregistratie af te mogen wijken. De dienst neemt de gegevens aangeleverd door de belastingplichtige als uitgangspunt als de laatstgenoemde aangeeft dat de GBA niet klopt (Tweede Kamer 2009-2010i). Minister De Jager merkte hierover in een Algemeen Overleg met de vaste Commissie voor Financiën op: "Het idee achter het GBA is heel goed, maar je ziet wel dat een onderdeel van de keten waarop de Belastingdienst zelf geen grip heeft, indirect toch uitstraalt op de dienstverlening van de Belastingdienst" (Tweede Kamer 2010-2011b: 11-12).

Wat zijn de kenmerkende doelstellingen van de diverse instrumenten in de gereedschapskist van de eOverheid? Een op ICT gebaseerde keten- of netwerkbenadering beoogt de verkokerde aanpak van verschillende organisaties te lijf te gaan, waardoor deze efficiënter en meer probleem- of vraaggestuurd kunnen werken (Expertcommissie informatievoorziening en elektronische dienstverlening SUWI 2005; Van Duivenboden et al. 2000; Grijpink 2006a). Digitale dossiers faciliteren de uitwisseling van gegevens, zoals bij de uitwisseling van indicatiegegevens tussen het UWV, het UWV-werkbedrijf, CIZ, MEE[12] en de gemeentelijke organisatie, in het kader van de Wmo, AWBZ, Wajong, WSW en WIA.[13] Koppelvlakken, verwijsindexen en landelijke schakelpunten zijn instrumenteel in het verbinden van de versplinterde wereld van tienduizenden lokale databanken en evenzovele elektronische dossiers die zijn gehuisvest in ontelbare publieke en semipublieke organisaties. Het EPD is zo'n landelijk schakelpunt. Via dit schakelpunt kan de informatie die bij verschillende zorgverleners beschikbaar is, worden opgevraagd op het moment dat een geautoriseerd persoon daarom vraagt (Pluut 2010). Het EPD is dus geen centraal opgeslagen digitaal dossier, maar een infrastructuur voor uitwisseling van informatie. Het EPD en andere infrastructuren maken gebruik van het BSN. Dit BSN moet als uniek, algemeen en informatieloos persoonsnummer burgers kunnen identificeren in hun relatie met de overheid (Tweede Kamer 2005-2006a). Het is daarbij ook nog eens een ordeningsnummer om gegevensbestanden binnen de overheid te ontdubbelen en de sleutel tot het stelsel van basisgegevens en authentieke registraties. "Het gebruik van het BSN voor opsporingsdoeleinden staat nog niet hoog op de beleidsagenda, maar zal ongetwijfeld met stip stijgen", zo merkte Het Expertise Centrum enkele jaren geleden al op (HEC 2007: 70). Met behulp van de authentieke registraties en basisgegevens ten slotte wordt gegarandeerd dat er één eenduidige en gezaghebbende bron van informatie is die ten dienste staat van allerhande samenwerkingsverbanden en ketens binnen de overheid (Tweede Kamer 2000-2001b). De kerngedachte

achter de basisregistraties is dat op uitvoeringsniveau gegevens slechts eenmalig verzameld worden bij burgers en bedrijven, gekoppeld aan een verplicht gebruik binnen de overheid. Deze basisadministraties worden als noodzakelijke voorwaarde gezien voor administratieve lastenverlichting, publieke dienstverlening, fraudebestrijding, interne efficiency van het overheidsapparaat en de beschikbaarheid van beleidsgegevens. Inmiddels spreekt men over het *stelsel van basisregistraties*[14], waarmee wordt aangegeven dat de basisregistraties juridisch, informatiekundig, technisch en organisatorisch zo afgestemd en gekoppeld worden dat ze overheidsbreed gebruikt kunnen worden. Ze vormen daarmee de 'ruggengraat' van de informatiehuishouding van de overheid.[15] Basisregistraties zijn databanken met juridisch bindende feiten over een groeiend aantal objecten van overheidssturing (burgers, auto's, panden, straten, enz.). Deze feiten worden als basisgegevens in meer en meer overheidsapplicaties ingelezen en daarmee door een toenemend aantal publieke instanties gebruikt. In principe biedt het stelsel van basisregistraties ook een uitgelezen kans voor het versterken van de positie van burgers, onder meer omdat de registraties ook zo kunnen worden ingericht dat burgers gemakkelijker zelf wijzigingen kunnen aanbrengen in deze registraties, aanvragen kunnen doen of bepaalde rechten claimen. Tot op heden benut de overheid dit emancipatoire potentieel van basisregistraties echter onvoldoende (Boschker, Castenmiller & Zuurmond 2010: 97-98).

De gereedschapskist van de eUitvoering is al met al een uitdijend geheel van technische faciliteiten zoals databanken en gestandaardiseerde informatie zoals unieke nummers. Belangrijke thema's hierbij zijn de standaardisatie, normalisatie en (semantische) interoperabiliteit[16] van al deze faciliteiten (College en Forum Standaardisatie 2009). Om alle onderdelen van de gereedschapskist naadloos op elkaar aan te sluiten zijn ambities, bouwstenen en afspraken neergelegd in het NUP (Nationaal Uitvoerings Programma Dienstverlening en e-Overheid) en NORA (Nederlandse Overheids Referentie Architectuur) en is wat betreft interoperabiliteit een sturende en faciliterende rol weggelegd voor het Bureau en Forum Standaardisatie (Forum Standaardisatie 2010). Hierin zijn deskundigen en betrokkenen vanuit overheid en bedrijfsleven verenigd. Het Forum fungeert als denktank voor het op hoog ambtelijk niveau neergelegde College Standaardisatie. Dat het met de ontwikkeling van sommige onderdelen uit de gereedschapskist overigens uiterst moeizaam gaat, bleek voorjaar 2010 toen de vernietigende Gateway Review NUP, uitgevoerd onder voorzitterschap van Docters van Leeuwen, naar de Tweede Kamer werd gezonden (Gateway NUP 2009).

4.1.4 EEN VERANDERENDE ADMINISTRATIEVE WERKELIJKHEID

Stap voor stap, soms snel en dan weer met vallen en opstaan, verandert de informatiehuishouding van de overheid. Juist op uitvoeringsniveau waar organisaties over het algemeen dichter bij burgers staan en regelmatig met hen in contact

moeten treden, wordt daarmee ook zichtbaar hoe deze nieuwe informatiehuishouding de relatie met en positie van burgers verandert. Eind jaren tachtig al voorzag Frissen dat databanken verworden tot "het 'archimedisch middelpunt' van waaruit planning van maatschappelijke collectiviteiten plaatsvindt" (Frissen 1989: 260). Tien jaar later concludeerde Van Duivenboden op basis van onderzoek naar koppelingspraktijken bij de Gemeentelijke Sociale Dienst (GSD) en de Rijksdienst voor het Wegverkeer (RDW) dat deze praktijken bij beide organisaties een verschuiving van de bewijslast van de overheidsinstantie naar de burger teweegbrengen (Van Duivenboden 1999: 322). Zo verplaatst bij het koppelen door de RDW de bewijslast "in de richting van de voertuigeigenaar, die zelf naar de GBA, de Belastingdienst of zijn verzekeringsmaatschappij zal moeten stappen. (…) In die zin is er een relatie tussen het opbouwen en verder uitbouwen van een virtueel register en een toename van de verantwoordelijkheid van de burger voor het herstellen van foutieve registratie" (Van Duivenboden 1999: 229). Rapporten van de Nationale Ombudsman over de vergelijking door de RDW van het kentekenregister, het verzekeringsregister en het APK-register "teruglopend van heden naar uiteindelijk januari 1995" bevestigen deze ontwikkeling (Nationale Ombudsman 2008; Nationale Ombudsman 2009b). Nog eens tien jaar later stelt Overkleeft-Verburg op basis van jurisprudentie vast dat rechters inderdaad meer en meer zijn geneigd om bij gebruik van een verkeerd gegeven het risico bij de burger neer te leggen (Overkleeft-Verburg 2009: 74). Ook in de Verenigde Staten lijkt er een beweging op gang waarbij de verantwoordelijkheid van de overheid en het bedrijfsleven in de richting van de individuele burger wordt geschoven, in dit geval bij identiteitsfraude (Whitson & Haggerty 2008). Maar er zijn meer veranderingen waar te nemen. Heel concreet resulteert de nieuwe inrichting van de informatiehuishouding namelijk ook in een splitsing van trajecten en verantwoordelijkheden over verschillende bestuursorganen: de eindverantwoordelijkheid voor het traject rondom het concrete besluit op een aanvraag van een burger (bijv. voor een uitkering) is met de introductie van basisadministraties losgekoppeld van het traject rondom de basisgegevens die voor dat besluit worden gebruikt. Voor de burger betekent het dat hij of zij in de huidige situatie met twee bestuursorganen te maken heeft, daar waar dat voorheen één instantie was.

Behalve met andere posities worden overheden en burgers ook geconfronteerd met nieuwe kwetsbaarheden. Kwetsbaarheden die voor de overheid variëren van een toenemend misbruik van systemen (Govcert.nl 2009: 9), een onvoldoende reflectie op digitale archivering tot het niet langer in staat zijn de gegevens in de (historische) context te plaatsen, gegevens op hun belang, kwetsbaarheid dan wel gevoeligheid te prioriteren of op hun juistheid te controleren. Illustratief in dit verband is een rapport van de Nationale Ombudsman over bestandsvergelijking tussen de Belastingdienst (zelfstandigenaftrek) en UWV (opgegeven uren) uitgevoerd ter controle van startende ZZP'ers. Op basis van die vergelijking bleek het fraudepercentage in de onderzoeksjaren 2007, 2008 en 2009 te variëren tussen

de 26 en 40 procent. Bijna 3000 zelfstandigen werden geconfronteerd met terugvorderingen, sancties en zelfs strafvervolging. Na onderzoek door de Nationale Ombudsman bleek dat de bestandskoppeling was uitgevoerd zonder oog te hebben voor de betekenis van de gegevens in hun individuele context. Een grote groep zelfstandigen bleek uiteindelijk ten onrechte beschuldigd van fraude (Nationale Ombudsman 2010b).

Voor burgers houden veel van de nieuwe kwetsbaarheden verband met het vernetwerken van informatie, i.e. het gezamenlijk gebruik en beheer van informatie in het netwerk van actoren dat tot stand komt via de genoemde ketens, koppelvlakken, verwijsindexen, enzovoorts. Deze vernetwerking wordt veelal aangemerkt als niets meer dan een technische exercitie. De consequenties gaan echter veel verder. Zoals eerder opgemerkt, worden vanuit de ketengedachte meer en meer organisaties via hun systemen vervlochten, daarbij sterk gefaciliteerd door het Burgerservicenummer (BSN). De techniek faciliteert de dwarsverbanden en maakt zo informatiestromen tussen organisaties mogelijk. Structurele dwarsverbanden in termen van verantwoordelijkheden en aansprakelijkheden blijven echter vaak achterwege. Kortom, semantiek op juridisch niveau houdt geen gelijke tred met semantiek op technisch niveau. Deze observatie is ook terug te vinden in de recente – tweejaarlijkse – trendrapportage van de overheid over ontwikkelingen in het decentrale bestuur: samenwerking neemt een grote vlucht, maar de gemeenschappelijke noemer bij de samenwerking is dat partijen hun beleidsautonomie behouden (Ministerie van BZK 2010: 36). Aldus blijft verantwoordelijkheid institutioneel bepaald volgens de traditionele inrichting van het openbaar bestuur.

Het gevolg is een versplintering van verantwoordelijkheid rondom informatieprocessen (verschillende actoren verantwoordelijk voor separate onderdelen van de keten) of zelfs een de facto 'verdwijnen' van verantwoordelijkheid, omdat verschillende partijen niet anders kunnen dan naar elkaar doorverwijzen, waar de informatietechnologische slag die is gemaakt simpelweg niet in verantwoordelijkheden is vertaald. Het gebruik van technologie en de ambitie om (beleids)informatie over burgers in ketens te organiseren, botst kortom met de traditioneel hiërarchisch georganiseerde overheid. Technisch en praktisch werkt men vaak al in ketens (of netwerken), maar besluitvorming, verantwoordelijkheidsverdeling, wetgeving en toezicht zijn daar nog niet op aangepast. Wat ontbreekt is een visie op het vraagstuk hoe coördinatie en verantwoordelijkheid georganiseerd moeten worden als informatie in netwerken en ketens van overheidsorganisaties rondgaat (Borst 2009: 262). Wat eveneens ontbreekt, aldus diverse betrokkenen, is doorzettingsmacht van een organisatie bij problemen als identiteitsfraude en situaties waarin geen enkele organisatie zijn verantwoordelijkheid voor problemen en fouten in de geketende systemen wenst te nemen. Zo is te lezen in een studie van het HEC over situaties waarin burgers door het gebruik van een BSN in de knel komen.

"Er zijn bij ons weten tussen de ministers die betrokken zijn bij uitvoeringsregelingen die gebruikmaken van het BSN, geen specifieke beleidsafspraken gemaakt om hier alert op te zijn of een functionaris aan te stellen die dergelijke gevallen op een gezaghebbende manier aan de orde kan stellen en de betreffende burger kan bijstaan. De in de Wet algemene bepalingen burgerservicenummer genoemde Functionaris Gegevensbescherming heeft volgens ons hiertoe noch de positie noch de bevoegdheden" (HEC 2007: 68).

4.1.5 MEER DAN EFFECTIVITEIT EN EFFICIËNTIE ALLEEN

Uiteindelijk moeten de ambities en het nieuwe gereedschap bijdragen aan betere dienstverlening, controle en zorg. Hoe en op basis van welke criteria de omvang van die bijdrage gemeten moet worden blijkt echter ook op uitvoeringsniveau geen sinecure. Moeten de resultaten langs de meetlat van effectiviteit en efficiëntie worden gelegd, of vormt de veel bredere set criteria zoals geformuleerd in de 'BurgerServiceCode' het meetinstrument?[17] De staatssecretaris van BZK merkte in 2007 over de rol van de 'BurgerServiceCode' op: "Het is dus één van de meetinstrumenten die wij kunnen gebruiken. Of en hoe we dat moeten doen, moet ik nog bekijken" (Burger@Overheid.nl 2007: 94). De nieuwe technologische mogelijkheden kunnen een sterke efficiëntie-impuls geven, waarbij in het meest gunstige geval wat efficiënt is voor de overheid overeenkomt met wat efficiënt is voor de burger. Hakkenberg, directeur van de RDW en tevens voorzitter van de Manifestgroep, wees op de voordelen voor zowel burgers als de overheid van de zogenaamde Berichtenbox (beschikbaar via mijnoverheid.nl).[18] Wanneer burgers dat op prijs stellen, communiceren de deelnemende uitvoeringsinstanties niet langer via papier, maar uitsluitend digitaal via deze Berichtenbox. De faciliteit biedt burgers niet alleen informatie- en transactiemogelijkheden, maar ook een eigen archieffunctie. Per jaar sturen uitvoeringsinstanties 600 miljoen brieven; als 100 miljoen daarvan niet meer per post worden verstuurd, betekent dat naast een nieuwe dienstverlening voor burgers ook een enorme kostenbesparing. Illustratief voor een opgepakte kans is ook de website van de RDW, die, mede in overleg met een gebruikersgroep, is ingericht naar doelgroepen en vanuit het perspectief van de klant. De website wordt inmiddels dertig miljoen keer per jaar bezocht. Vooral de transactiemogelijkheden via de web-selfservice blijken populair bij burgers. Het bespaart hen kosten en is zeven dagen per week en 24 uur per dag beschikbaar. Nu bijvoorbeeld het schorsen van een voertuig via het internet kan, is het aantal schorsingen met 40-50 procent toegenomen. Ook aan inzage in de eigen gegevens blijkt een enorme behoefte te bestaan, aldus Hakkenberg. Ten slotte kan het volgende bericht in het Jaarverslag 2008 van de Informatie Beheer Groep (IB-Groep) als voorbeeld dienen.

"In 2008 hebben klanten 2,9 miljoen keer op Mijn IB-Groep ingelogd voor informatie over hun gegevens. In meer dan 600.000 gevallen is hierbij een digitale wijziging doorgevoerd. Daarnaast konden studenten via Mijn IB-Groep in 2008 voor het eerst aangeven of ze hun studiefinancieringsberichten digitaal wilden ontvangen. Hierdoor zijn 375.000 berichten digitaal verstuurd in plaats van via de post. Ook zijn in 2008 voor het eerst proactieve e-mails, met informatie op maat, gestuurd aan gebruikers van Mijn IB-Groep. De IB-Groep heeft bijvoorbeeld aanstaande studenten in het hoger onderwijs die zich al wel hadden aangemeld voor een opleiding maar nog geen studiefinanciering hadden aangevraagd, daarop via een e-mail geattendeerd"(IB-Groep 2009: 20).

Maar behalve aandacht voor stuwende beginselen wordt er op uitvoeringsniveau ook waarde gehecht aan verankerende beginselen zoals privacy. Alhoewel privacy niet in iedere context belangrijk wordt gevonden (Zenc 2007: 77) en zowel het CBP als de Nationale Ombudsman met een zekere regelmaat wijzen op schendingen van privacy door uitvoeringsinstanties, staat privacy bij vooral grote uitvoeringsinstanties wel degelijk op het netvlies. Van Duivenboden constateerde jaren geleden al op basis van onderzoek naar koppelingen bij de Gemeentelijke Sociale Dienst en RDW dat privacy de aandacht van deze organisaties had (Van Duivenboden 1999: 234). Daar waar uitvoeringsinstanties privacy expliciet in het vizier hebben, valt dit deels terug te voeren op het feit dat deze instanties relatief dicht bij burgers staan en regelmatig direct met hen in contact moeten treden. Soms ook is privacy een expliciet element in de *business case* voor een nieuwe e-dienst, juist omdat maatschappelijke acceptatie van belang is voor het slagen van het initiatief. Uit het onderzoek van Van Duivenboden bleek dat er een relatie was te leggen tussen de strijd tot behoud van autonomie enerzijds en zorgvuldigheid in de omgang met persoonsgegevens anderzijds: "Bovendien ondersteunt ook de wens van de GSD zijn autonomie zoveel mogelijk te behouden, het maken van precieze afspraken over wie welke gegevens mag inzien of ontvangen en andersom" (Van Duivenboden 1999: 178). Deze constatering is van belang, nu de populariteit van het werken in netwerken, ketens en via schakelpunten op een afbrokkeling van privacy lijkt te wijzen. De gesprekspartners van de WRR merken op dat netwerken en ketens op het snijvlak van publiek en privaat worden verknoopt, maar dat het ontbreekt aan adequate toezichtarrangementen om het verdere gebruik door de private sector van de vanuit de publieke sector verstrekte gegevens te controleren. Zo merken Tankink en Van Dongen van het Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) het volgende op.

"De GBA verstrekt vanwege publieke taken gegevens aan uitvoeringsinstellingen als pensioenverzekeraars, APK-keurders en deurwaarders. Maar deze actoren voeren naast hun publieke taken, ook private taken uit. Waar de procedure voorafgaand aan verstrekking van de gegevens strikt is vormgegeven met behulp van logging, is de controle wanneer gegevens eenmaal zijn verstrekt beperkt en ontbreekt zicht op de doeleinden waarvoor de gegevens uiteindelijk worden gebruikt."[19]

Juist ook vanwege de variëteit aan ketenpartners blijken er in de praktijk diverse problemen te ontstaan rondom de zorgvuldige omgang met en kwaliteit van persoonsgegevens. De Nationale Ombudsman concludeert: "Keteninformatisering kan wellicht bepaalde bestuurlijke problemen oplossen en eventueel de vernieuwingsprocessen bij de overheid versnellen, maar er is weinig grond voor een al te groot vertrouwen in de invloed van keteninformatisering" (Nationale Ombudsman 2009a: 28).

De procesmatige beginselen van transparantie en accountability lijken op uitvoeringsniveau echter onder druk te staan. Hiervoor werd al gerefereerd aan de versplintering van verantwoordelijkheid of zelfs een de facto 'verdwijnen' van verantwoordelijkheid wanneer in netwerken en ketens wordt samengewerkt. Illustratief is de eerdergenoemde kwestie rond de sociale recherche die een groot aantal bestanden koppelt om risicoprofielen op te stellen. Het CBP wees de SIOD erop dat ze de betrokken burgers hierover had moeten informeren, waarna de SIOD te kennen gaf dit een taak van de regionale interventieteams te vinden. Deze teams geven immers de indicatoren door die de kans op het aantreffen van bijstandsfraude verhogen, aldus de SIOD (CBP 2010b). Maar ook transparantie, in de zin van transparantie voor democratische betrokkenheid en controle, blijkt problematisch. Al ten tijde van de ontwikkeling van de GBA, zo concludeerde Straten (1996: 254), heeft de politiek zich gemarginaliseerd. Zouridis (2000: 318) stelde op basis van studies bij de Informatie Beheer Groep (IB-Groep) en het Centraal Justitieel Incasso Bureau (CJIB) vast dat de systeemontwikkeling bij deze uitvoeringsorganisaties dermate omvangrijk en complex is dat de politieke betrokkenheid erbij minimaal te noemen valt. "Heeft wetgeving wel de sturende en richtinggevende rol die het primaat van de wetgever en dat van de politiek veronderstellen? Is wetgeving langzamerhand niet ook een afgeleide geworden of het resultaat van interacties met de organisatie en ICT?" (Zouridis 2000: 318). Het antwoord op deze vragen klemt des te meer, omdat Zouridis constateert dat er gaten vallen in de organisatie van de verantwoording van systeemontwikkeling: "Hoe transparant is het algoritme in het geautomatiseerd systeem bijvoorbeeld? In de casus van de studiefinanciering is gesproken over een systeem met 'puisten en pukkels', dat zelfs voor insiders al lastig te begrijpen is (…)" (Zouridis 2000: 315). Het traject bij de Verwijsindex Risicojongeren laat bovendien zien dat het wetgevend fundament veelal pas wordt gelegd als de projecten al lang op stoom zijn en daarmee de inrichting (welke gegevens worden opgenomen, wie mag de gegevens aanleveren, wie mag ze inzien, met welke andere initiatieven wordt gekoppeld, enz.) al lang concreet is bepaald (Keymolen & Prins 2011).

4.2 LOKALE WORSTELINGEN

Op 28 oktober 2009 stelde de Raad van Hoofdcommissarissen het visiedocument over cameratoezicht, getiteld *Beelden van de Samenleving*, vast. Het voor-

woord schetst de knelpunten en dilemma's waar de politie zich voor gesteld ziet.

"[H]et publieke en private cameratoezicht vertoont tot op heden onvoldoende professionaliteit en samenhang. Daarnaast neemt het gebruik van intelligente cameratoepassingen door publieke en private partijen toe, waarbij bijvoorbeeld waarnemingen en registraties van personen en voertuigen worden vergeleken met uiteenlopende databestanden. De vraag die zich aandient, is waar straks de grens ligt. De zoektocht naar voor veiligheid waardevolle data en de mogelijkheden die de techniek biedt, brengen het risico dat ongebreidelde grote hoeveelheden (en vaak onnodige) informatie worden verzameld en gekoppeld. Dit is vanuit privacyoogpunt onwenselijk" (Raad van Hoofdcommissarissen 2009: 3).

Op lokaal en regionaal niveau zijn het met name de gemeenten en politiekorpsen die een belangrijke spilfunctie hebben als het gaat om de inzet van ICT. Kenmerkend voor de dynamiek die zich op dit niveau openbaart, is hun relatief autonome optreden, waardoor een uiterst gevarieerd landschap aan initiatieven en daarbij horende praktijken en randvoorwaarden te ontwaren valt. Kenmerkend is echter ook de heel tastbare worsteling van deze actoren tussen enerzijds het enthousiast oppakken van de ongekende nieuwe kansen die digitalisering biedt voor het uitvoeren van de eigen taken en anderzijds de grenzen die er ook in hun ogen moeten zijn aan het benutten van de kansen. Veel van de lokale gesprekspartners van de WRR uitten hun onvrede en frustratie over de afwezige helpende hand vanuit Den Haag bij het maken van de noodzakelijke keuzes. Deze gepercipieerde afwezigheid geldt een scala aan Haagse instanties, variërend van de Vereniging Nederlandse Gemeenten (VNG) en het College Bescherming Persoonsgegevens tot de verantwoordelijke departementen. Dit beeld is ook terug te vinden in de eerdergenoemde Gateway Review NUP.

"Veel respondenten hebben bovendien specifiek kritiek op de te weinig proactieve houding van de VNG in het traject tot nu toe en ook op de geringe profilering van de VNG ten aanzien van onderwerpen die gezamenlijkheid en standaardisatie veronderstellen. Dezelfde kritiek geldt mutatis mutandis voor het ministerie van BZK als 'coördinerend' departement" (Gateway NUP 2009).

4.2.1 GEMEENTEN 2.0

Gemeenten innoveren vanuit hun eigen ambities met ICT (bijv. digitale volgsystemen voor vergunningsverzoeken, nieuwe concepten voor de gegevensmagazijnen in de backoffices), maar zijn vooral een belangrijke partij bij de uitvoering van diverse landelijke ambities. Die ambities lagen in eerste instantie bij digitale dienstverlening, met initiatieven als e-formulieren, gepersonaliseerde webfuncties via mijnoverheid.nl, aansluiting voor gemeentelijke diensten op DigiD, de

vernieuwing van de GBA in combinatie met de introductie van authentieke registraties en basisgegevens en recent het Antwoord© initiatief, waarbij de (digitale) gemeente als *het* aanspreekpunt wordt aangemerkt voor het juiste antwoord op de meest gestelde vragen van burgers.[20]

Maar de gemeente speelt meer recent ook een belangrijke rol bij de uitvoering van ICT-initiatieven op het terrein van controle (uitgifte van paspoorten en daarmee de toepassing van biometrie) en zorg en controle (de Verwijsindex Risicojongeren en het Veiligheidshuis). Daarbij wordt duidelijk dat ook op lokaal niveau de grenzen op meerdere fronten gaan schuiven. Allereerst geldt dat voor de grenzen tussen verschillende beleidsdomeinen. Zorg krijgt een controlecomponent, zoals bij de Verwijsindex Risicojongeren. Ten tweede schuiven ook hier de grenzen tussen publieke, semipublieke en private sector. In het initiatief voor een Landelijk Informatiesysteem Schulden (LIS), waarmee de schuldenproblematiek wordt aangepakt, participeren niet alleen gemeenten (gemeentelijke sociale dienst), maar ook energiebedrijven, woningcorporaties, leden van de Nederlandse Vereniging voor Volkskrediet en het Leger des Heils (LIS 2009). Bij het overleg binnen het Veiligheidshuis kunnen instellingen aansluiten die zich daarvoor niet eerder zo centraal in het domein van zorg voor risicojongeren bevonden, zoals kinderopvang, speelpleinen, kredietbanken, Leger des Heils en naschoolse opvang, en daarmee zeggenschap verkrijgen buiten het domein waarin ze van oudsher opereren (Holvast & Bonthuis 2010: 32-33). Lokale overheden zetten in toenemende mate particuliere cameratoezichtcentrales in ten behoeve van handhaving van de openbare orde. Bovendien blijkt dat in een kwart (24%) van de gemeenten de kosten voor cameraprojecten worden gedragen door gemeente en particuliere ondernemingen gezamenlijk (Schreijenberg et al. 2009). Al deze private partijen krijgen daarmee de rol van ‘deputy sheriffs’ (Torpey 2000; Lahav & Guiraudon 2000), in wat wel “nodale veiligheidszorg” wordt genoemd (Rozemond 2010; Boutellier 2007).

Geautomatiseerde ‘professionaliteit’

Veelal geen doelstelling op rijksniveau maar wel op lokaal niveau is het genereren van managementinformatie met behulp van de ICT-initiatieven. Duidelijk is deze tendens zichtbaar bij de Verwijsindex Risicojongeren, waar op lokaal niveau het systeem ook wordt ingezet als middel voor procesbewaking en het onderlinge toezicht van hulpverleners (Keymolen & Broeders 2010; Keymolen & Prins 2011). Professionals zijn bij te sturen en processen of diensten vallen af te rekenen op de mate waarin ze rendabel zijn, op basis van managementinformatie die door de verschillende databanken – van de OV-chipkaart tot de Verwijsindex Risicojongeren – wordt gegenereerd. De handelingsruimte van uitvoerende ambtenaren en professionals (professionele autonomie) staat ook onder druk wanneer keuzes en beslissingen die professionals moeten nemen over en voor burgers, belastingbetalers, patiënten, enzovoorts worden beïnvloed en bepaald door profielen en auto-

matisch gegenereerde beelden die de overheid van haar burgers heeft. Zuurmond heeft deze ontwikkeling vanuit een sociologisch perspectief geduid als infocratie (Zuurmond 1994). Bovens en Zouridis (2002) spreken van een ontwikkeling waarbij beslissingsmacht verschuift van de *street level bureaucrat*, via de *screen level bureaucrat* naar uiteindelijk de *system level bureaucrat*. Zuurmond en Meesters (2005) stellen dat in een netwerkomgeving deze *system level bureaucrats* op hun beurt weer worden verdrongen door de *chain level bureaucrats* – de personen die met een grote discretionaire ruimte bepalen hoe de informatiesystemen en processen van het netwerk eruitzien. Lyon (2009) spreekt in de context van identificatie en ID-kaarten van *stretched screens*, een observatie die ook van toepassing is op de medewerkers van de Belastingtelefoon en Postbus 51 (Nationale Ombudsman 2010a). Zij hebben zich in het gesprek met burgers te houden aan de informatie getoond op het computerscherm. Professionele autonomie, keuzevrijheid en de menselijke maat komen hiermee onder druk te staan, wat als het ware leidt tot een kwetsbaarheid op 'straatniveau'. Veel ambtenaren en andere professionals die met de ICT-systemen van de overheid te maken krijgen (zoals de artsen met het EPD) functioneren op dit 'straatniveau'. Waar burgers zich door technologie vervreemd kunnen voelen, geldt dit natuurlijk evenzeer voor professionals. De kwetsbaarheid toont zich hier niet als systeemuitval maar als ondoorzichtige en onvoorspelbare 'uitval' binnen sociale contexten, waar systemen een onbedoelde werking hebben, die disfunctioneel is, dan wel waar professionals zich aan de technologische inkapseling van hun metier proberen te onttrekken (Van den Akker & Kuiper 2008). Zo mogen artsen naast het 'officiële' dossier, waarvoor een verplichting bestaat tot uitwisseling via het landelijk schakelpunt, ook schaduwdossiers bijhouden met meer uitgebreide werkaantekeningen.

Gemeentelijk onvermogen

De veelheid aan mooie plannen en ambities vertroebelt vaak het zicht op de worsteling van veel gemeenten met de eOverheid. Zo was 11 procent van de gemeenten per 1 juni 2010 nog niet aangesloten op de basisadministratie personen (GBA), terwijl het gebruik hiervan al vanaf 1 januari 2010 verplicht was (Tweede Kamer 2009-2010a). Bovendien bleek 32 procent van de afnemers nog niet gereed te zijn voor aansluiting en bleek 5 procent van alle burgers op een onjuiste wijze in de GBA geregistreerd te staan, wat heel concreet neerkomt op 800.000 foutief geregistreerde burgers. Maar gemeenten lopen ook tegen vraagstukken aan die de traditionele inrichtingsprincipes van het openbaar bestuur raken. De sterke nadruk op digitale dienstverlening-op-maat leidt tot spanningen in de gemeentelijke organisatie, omdat de dagelijkse praktijk van klantgericht werken botst met traditionele waarden en opvattingen in het openbaar bestuur (Hoogwout 2010). Bovendien wringt de digitale ondersteuning van dit klantgerichte denken met de wettelijke regimes voor de omgang met persoonsgegevens. Klantgericht denken dwingt gemeenten namelijk de gegevenshuishouding op de schop te nemen en een nieuw inrichtingsmodel te ontwikkelen, het zogenaamde Midoffice. Dit

Midoffice moet de schakel worden tussen het klantcontactcentrum van een gemeente (het 'ene loket') en het scala aan backofficesystemen waar alle benodigde gegevens uit opgehaald moeten worden. Behalve een hoop (financiële) ellende en systeemontwikkelingsperikelen (Mom 2010) heeft de introductie van het Midoffice op een meer fundamenteel niveau tot gevolg dat zonder een zorgvuldige discussie nu voor meer werkzaamheden en taken informatie uit het gegevensmagazijn wordt opgehaald dan wettelijk is toegestaan.[21] Uiteindelijk blijken de kleine en sommige middelgrote gemeenten vanwege beschikbare financiën en deskundigheid nauwelijks in staat de complexe technische en inhoudelijke materie te hanteren en zich om te vormen naar de eOverheid. Maar ook bij grote gemeenten gaat het niet soepel. Najaar 2010 kwam in Amsterdam de overboeking van uitkeringen door de sociale dienst in gevaar vanwege een crisis bij de gemeentelijke ICT.

Het CapGemini rapport *Puzzelen met prioriteit* (Van Duivenboden & Rietdijk 2005) ziet als belangrijkste verklaring voor problemen dat de eOverheid wordt beschouwd als een technologische aangelegenheid die thuishoort bij afdelingen Informatisering & Automatisering (I&A) of bij de bedrijfsvoering. Beleidsmensen onderkennen de maatschappelijke implicaties van de inzet van technologie niet en staan niet stil bij de bredere condities en het raamwerk. Ze vinden het moeilijk om het politieke discours te vertalen naar techneuten, maar I&A-mensen zijn op hun beurt niet in staat om technische specificaties te vertalen naar de sociaal-politieke context. Dit onvermogen is een gat waar de consultants inspringen, aldus zowel het rapport als gesprekspartners van de WRR.[22] Aanvullend geven deze aan dat lokaal het wiel te vaak opnieuw moet worden uitgevonden en er, als het om goed opdrachtgeverschap gaat, weinig sturing vanuit rijksniveau of de VNG is. Zo uit de voorzitter van de Manisfestgroep, Hakkenberg[23], zich in kritische zin over de ambitie, in 2005 geformuleerd door de commissie-Jorritsma, om gemeenten vanaf 2015 ook langs digitale weg het eerste aanspreekpunt te laten zijn als betrouwbare en herkenbare ingang voor de hele overheid. Het gaat hier om het concept *Antwoord©* (commissie-Jorritsma 2005): "Welk kanaal burgers en ondernemers ook kiezen, het ene telefoonnummer, de gemeentelijke website of de balie, zij krijgen steeds hetzelfde betrouwbare antwoord op vragen, het in gang zetten van aanvragen en doorverwijzen naar andere overheidsorganisaties."[24] Hakkenberg merkt vanuit eigen ervaringen op dat het volstrekt onrealistisch is te verwachten dat gemeenten de hiervoor benodigde gigantische digitale kennisbank kunnen opbouwen, laat staan beheren, onderhouden en via één loket communiceren met burgers.

Afwezige helpende en sturende hand

Uiteindelijk heeft het lokaal onvermogen consequenties voor de inrichting van en democratische controle op de bredere ontwikkeling van de eOverheid. Of het nu gaat om landelijk digitaliseringsbeleid met (gedeeltelijk) vanuit het rijk aangestuurde projecten, om landelijk sectoraal beleid waarbij systemen een ondersteunende rol spelen, of om de eigen gemeentelijke innovatieambities met de informatiehuis-

houding, de gemeente opereert vrijwel altijd in een context waarin verschillende beleidsdomeinen elkaar raken en waarbij vele partijen betrokken zijn. Dit maakt dat juist op lokaal niveau aandacht voor de bredere context waarin de applicaties vorm en inhoud krijgen, het borgen van verantwoordelijkheden en realiseren van toezichtarrangementen tot de belangrijke aandachtspunten zouden moeten behoren. De realiteit toont echter een beeld van een enorme diversiteit aan lokale initiatieven, gecombineerd met de variëteit aan betrokken publieke en private actoren, wat adequate controle, toezicht en handhaving belemmert. Veiligheid blijkt op lokaal niveau een stuwend beginsel van betekenis te zijn, vaak ten koste van privacy. Illustratief is het enthousiasme van een medewerker van het Veiligheidshuis Amsterdam over de inzet van een zoekprogramma genaamd Topic View.

"Topic View is uniek (...) Het geeft ons iedere dag alle informatie uit alle politiebestanden. Niet alleen uit officiële stukken, maar ook uit Wordbestanden die de politie even snel heeft ingevoerd. Topic View bevat ook 'zachte informatie'. Iemand rijdt in een dure auto, maar het gezin heeft schulden. Vroeger zouden we iets aan de schulden doen. Nu gaan we op zoek naar de illegale financieringsbron. Een informatiespecialist verwerkt de informatie en op basis daarvan zetten we een informatieopdracht uit" (Holvast & Bonthuis 2010: 34).

Het toezicht vanuit het CBP op deze en andere lokale praktijken blijkt echter nauwelijks aan de orde. De gang van zaken rondom de Verwijsindex Risicojongeren laat zien dat als het ware twee werkelijkheden in ontwikkeling zijn: de wereld van de tekentafel op rijksniveau waar een systeem omschreven en wettelijk verankerd wordt, en de wereld van de werkvloer op lokaal niveau waar niet alleen een technisch systeem, maar ook de achterliggende informatieprocessen inhoudelijk vorm krijgen. De afwegingen die aan de tekentafel gemaakt zijn, de aandacht die is besteed aan de consequenties voor burgers, zijn nauwelijks bepalend voor de verwijzingssystemen die op de werkvloer tot stand komen. Daar voeren de stuwende beginselen ongehinderd de boventoon (Keymolen & Prins 2011).

De vraag dient zich hiermee aan naar de gewenste mate van coördinatie en sturing vanuit rijksniveau. Het tableau van worstelingen, eigengereide benutting van kansen, versplintering van toepassingen en het gebrek aan democratische controle hangt voor een belangrijk deel samen met de 'Nederlandse bestuurscultuur'. Besluiten kunnen niet eenvoudig aan gemeenten worden opgelegd, invloed kan moeilijk worden uitgeoefend en het daardoor soms noodzakelijke bestuursakkoord betekent langdurige procedures. Alhoewel het kabinet inmiddels uitvoering geeft aan suggesties van de commissie-Oosting ter verbetering van het interbestuurlijk toezicht, varen gemeenten bij digitalisering en informatieprocessen vaak hun eigen koers (breed EKD in plaats van de door de minister gepropageerde beperkte variant), dan wel bepalen hun eigen invoeringstempo. Veel gemeenten werken bij de elektronische dienstverlening aan burgers nog met gebruikers-

naam/wachtwoord, terwijl deze per 1 juni 2009 vervangen hadden moeten zijn door DigiD. En naar verluid zijn er zelfs nog gemeenten die niet met de GBA, maar met hun eigen bevolkingsadministratie werken. Via Versnellingsagenda's en andere initiatieven probeert de rijksoverheid te sturen en druk uit te oefenen, maar het Huis van Thorbecke blijkt op gespannen voet te staan met de digitaliseringsambities van de rijksoverheid. Ondertussen groeit ook op gemeentelijk niveau een wereld van verbonden systemen en informatieprocessen. Zo zijn alle lokale systemen voor de Verwijsindex Risicojongeren via een landelijke kop – paraplu – onderling met elkaar verbonden, om zo een 'dekkende' signalering van risicojongeren voor het gehele land te realiseren. Het is dan ook opvallend dat het fenomeen van digitalisering niet of nauwelijks figureert in het actuele debat over de herinrichting van het openbaar bestuur. Zo rept de discussienota van de VNG, die nota bene de veelzeggende titel *Thorbecke 2.0* draagt, met geen woord over de invloed van ICT op de verhoudingen in bestuurlijk Nederland (VNG 2010). En de Rob (2010b: 25) kaart weliswaar kenmerkende eigenschappen van de eOverheid aan, zoals horizontalisering en versplintering, maar brengt ICT en automatisering alleen expliciet in verband met de problematische kennislacune van gemeenten nu ze ieder voor zich een interactieve en dienstverlenende website moeten hebben.

4.3 INFORMATIEGESTUURDE POLITIE

4.3.1 STRATEGISCHE ORIËNTATIE EN PRAKTIJK

Tal van korpsoverstijgende programma's hebben de afgelopen jaren vorm en inhoud gegeven aan de digitaliseringsslag binnen de politieorganisatie: meer garanties voor een integer persoonsbeeld via de inzet van biometrie, slimme controles op knooppunten van wegen, havens, stations (de zgn. nodale oriëntatie[25]), het benutten van open informatiebronnen als Hyves en Facebook voor opsporingsdoeleinden en meer inzet van ICT voor analyse en verrijking van informatie. En ook hier is de omslag naar vroegtijdig en toekomstgericht handelen (preventie) zichtbaar: "De ontwikkeling die is ingezet van Informatiegestuurde *opsporing* naar Informatiegestuurde *politiezorg* (IGP) wordt verder uitgebouwd", aldus de Raad van Hoofdcommissarissen in 2005 (2005: 17). Individuele korpsen op lokaal en regionaal niveau spelen een essentiële rol bij het uitvoeren van de plannen en ambities. Maar evenals gemeenten blijken ook lokale korpsen te worstelen met de landelijke ambities en in wezen ook met hun autonomie bij het uitvoeren maar ook ontwikkelen van eigen initiatieven.

Zo hapert de geïntegreerde aanpak voor het vergaren van inzicht in en het bestrijden van identiteitsfraude binnen politiesystemen, en wijzen korpsen naar elkaar als een burger foutieve gegevens uit de systemen verwijderd wil hebben (Buruma 2011). De enkele jaren geleden met veel media-aandacht gelanceerde 'virtuele slotgrachten'[26] komen nauwelijks van de grond vanwege problemen bij lokale korp-

sen. Een onderzoek in opdracht van de Politieacademie naar de ervaringen met de in 2005 door de Raad van Hoofdcommissarissen gelanceerde 'nodale oriëntatie' is kritisch en concludeert dat de werkvloer worstelt om de ambities van de politietop in de dagelijkse praktijk handen en voeten te geven (Ferwerda et al. 2010). Er zijn inmiddels wel controles rond (vaar)wegen en treinstations die gericht zijn op het identificeren van grote aantallen weggebruikers, die zijn gebaseerd op samenwerking met niet-politiële diensten en waarbij geavanceerde meet- en zoekapparatuur wordt ingezet. Maar de ambities blijken lastig uitvoerbaar, gezien de hardnekkige focus op gebiedsgebonden politiewerk en bij gebrek aan concrete richtlijnen, aldus het rapport. In juli 2010 moest de verantwoordelijk minister aan de Tweede Kamer melden dat het op vele onderdelen slecht is gesteld met de informatiehuishouding van de politie. In niet mis te verstane conclusies constateert de minister begin juli 2010: "Er zijn grote risico's genomen bij de implementatie van de basisvoorzieningen waardoor de betrouwbaarheid en continuïteit van de informatievoorziening op het spel stonden. Het gemeentelijk functioneren van de Nederlandse politie is in dit opzicht niet verbeterd" (Tweede Kamer 2009-2010c: 2). Gesprekspartners van de WRR binnen de politie geven op hun beurt aan op korpsniveau het wiel te vaak zelf te moeten uitvinden en te weinig sturing c.q. steun vanuit rijksniveau te ondervinden bij de dilemma's op het terrein van gegevensverwerking en de aanpak van problemen rondom de kwaliteit van informatie. Als voorbeeld wordt gewezen op de participatie van de politie in de Verwijsindex Risicojongeren en de aanpak van identiteitsfraude. Zo zijn er al jaren spanningen tussen gemeente en politie over de aanpak van identiteitsfraude met paspoorten. Waar de gemeente wordt gemotiveerd door dienstverlening aan burgers, en burgers na verlies van een paspoort dus zo snel mogelijk van een nieuw exemplaar worden voorzien, wordt de politie geleid door handhaving en opsporing, waardoor ze een zeer restrictieve uitgifte van nieuwe paspoorten voorstaat. Eenzelfde soort spanning tussen dienstverlening en controle doet zich voor op luchthavens, tussen de marechaussee en de luchtvaartmaatschappijen (Snijder 2010). Zeker nu het paspoort is voorzien van biometrie achten de gesprekspartners het van groot belang dat via meer regie vanuit Den Haag op dit dossier wordt gestuurd.

4.3.2 SAMENWERKEN EN AFSTEMMEN MITS...

De initiatieven bij de politie laten zich duiden met dezelfde kenmerken als eerder besproken:

– op een technisch niveau krijgt vervlechting en verbinding in hoog tempo vorm, maar organisatorisch en politiek-bestuurlijk blijven de randvoorwaarden verschillend en de verantwoordelijkheden gescheiden,
– op informatieniveau worden grenzen diffuus, zowel wat betreft beleidsterreinen (service, care en control) als betrokken actoren (publiek – privaat) en
– ook hier blijkt sturing langs hiërarchische weg problematisch.

Box 4.1 Meesurfen: politie op het sociale web

Het groeiende gebruik van sociale media in de samenleving raakt ook het functioneren van publieke actoren als de politie en het OM. Er wordt – vooral 'van onderaf' – veel energie gestoken in het sociale web als communicatiestrategie en/of als forum voor opsporingswerk. De wijkagent die twittert, maakt zichzelf zichtbaar op een communicatiekanaal dat voor steeds meer 'cliënten' een belangrijk venster op de werkelijkheid is. De organisatorische risico's die een dergelijke informalisering behelzen, worden steeds meer voor lief genomen ten faveure van de directe band met burgers die zij bewerkstelligt. Een volgende variant van 'meesurfen' raakt al meer de kern van het politiewerk. In toenemende mate nodigen politie en justitie burgers uit om bij te dragen aan het opsporingswerk. Initiatieven als Burgernet (www.burgernet.nl) en de Hyves-pagina van het korps IJsselland (www.depolitiezoekt.hyves.nl) kunnen worden gezien als vormen van *crowdsourcing* in het politiewerk. Een gevolg van deze ontwikkeling is wel dat het doorploegen van een stortvloed aan vaak nutteloze tips onderdeel wordt van het rechercheren. Korps landelijke politiediensten (KLPD)-woordvoerder Ed Kraszewski benadrukte onlangs in een interview dat de hoeveelheid informatie die politieberichten opleveren, veel tijd kost en niet erg effectief blijkt voor het opsporen van een ontsnapte.[27] Hij stelt dat zijn dienst soms 'de regie kwijtraakt'over het eigen werk.

De echte goudmijn van informatie wordt echter niet door de politie zelf gegenereerd, maar door nietsvermoedende gebruikers van het web. Nagenoeg iedereen laat digitale sporen na van zijn relaties, gedrag, locatie enzovoorts. Als de politie dit domein betreedt, wordt 'meesurfen' des te pikanter, omdat gebruikers (verdachten maar ook anderen) dan de rekening gepresenteerd krijgen van het 'eeuwige geheugen van het internet' waarin zij stukjes van hun levenswandel hebben achtergelaten. Bijna alle politiekorpsen doen inmiddels mee met het Internet Recherche Netwerk,[28] waardoor is voorzien in *stand-alone* computers waarop politiemensen de gangen van personen kunnen nagaan zonder dat die dit hoeven te merken. Bovendien kunnen sociale netwerksites ook op een veel grotere schaal, en zonder een al te specifiek doel, 'geoogst' worden. Deze 'oogst' uit publieke bronnen wordt expliciet in het vooruitzicht gesteld door het Kecida,[29] een afdeling binnen het Nederlands Forensisch Instituut die zich specialiseert in intelligente data-analyse. Het is nog lang niet duidelijk binnen welke randvoorwaarden (waarborgen) deze vorm van 'meesurfen' heeft plaats te vinden: enerzijds wordt opgemerkt dat 'stelselmatig observeren' ook in de digitale wereld niet zomaar kan[30], maar anderzijds wordt ook nog veel gewicht toegekend aan het argument dat de digitale sporen die mensen achterlaten openbaar zijn (Buruma 2011).

Het resultaat wordt treffend verwoord in de observatie van de hoofdcommissarissen van politie als het over de inzet van particuliere cameratoezichtcentrales gaat: "De vraag is of er op deze wijze voldoende waarborgen zijn wat betreft kwaliteit, integriteit, democratische controle en voering in de regie van de overheid" (Raad van Hoofdcommissarissen 2009: 23). Als concrete illustratie kan ANPR dienen, het 'spontane' en inmiddels wijdverbreide initiatief van automatische kentekenherkenning. De politie zet deze cameratechniek in voor de handhaving van de openbare orde en opsporing van strafbare feiten, waarbij ze gebruikmaakt van vergelij-

kingsbestanden van gesignaleerde personen, gestolen voertuigen en openstaande boetes. ANPR is in korte tijd uitgebouwd met een rijkdom aan toepassingen: de politie zet het – overigens met wisselend goedvinden van de rechter[31] – in bij de aanpak van drugsrunnersproblematiek en bestrijding van mobiel banditisme. Samen met de politie gebruikt de VROM-inspectie de gegevens voor controles van afvaltransporten, gebruikt de Inspectie Verkeer en Waterstaat ze voor controle van het taxivervoer en controle op rij- en rusttijden, zet Rijkswaterstaat de gegevens in voor het in kaart brengen van verkeersstromen en gebruikt de Belastingdienst ze voor controle op verschillende belastingen (Eerste Kamer 2009-2010a). Niet alleen de variëteit aan toepassingen, en daarmee betrokken actoren, blijkt bij afwezigheid van enige specifieke (bij)sturing vanuit de politiek groot, dat geldt ook voor de termijnen voor het bewaren van de gegevens. "Het regiokorps IJsselland bewaart de gegevens zeven dagen, het korps Drenthe veertien dagen (...). Het korps Rotterdam-Rijnmond bewaart de gegevens vier maanden omdat ANPR ook wordt ingezet voor de opsporing, onder meer bij de bestrijding van drugssmokkel. Er zijn ook korpsen die langere termijnen hanteren" (Commissie Brouwer-Korf 2009: 68). Nadat een studie van Regioplan naar de meerwaarde van ANPR boven de A28 bij Zwolle concludeerde dat het systeem inderdaad specifieke opsporingsinformatie oplevert en bovendien informatie ('bijvangst') aanlevert die anders niet boven tafel was gekomen (Tweede Kamer 2010-2011f: 24-25), liet minister Opstelten van Veiligheid en Justitie begin december 2010 weten op korte termijn met wetgeving te komen. De regels moeten het ook mogelijk maken 'onverdachte' kentekens langer te bewaren.[32] Voor Kamerleden Schouw en Berndsen was deze mededeling aanleiding tot het stellen van een groot aantal vragen, waaronder over de kwetsbaarheid voor lekken en de inbreuk op de privacy van automobilisten (Tweede Kamer 2010-2011g: 1-2).

4.3.3 VERGETELHEID

Juist het breed verzamelen van informatie door de politie en in het verlengde daarvan justitie, heeft uiteindelijk ook gevolgen voor het concept van 'vergeten' in het digitale tijdperk en de eOverheid (Mayer-Schönberger 2009; Solove 2007; Buruma 2011). Technisch gezien is een recht op vergeten en daarmee 'opnieuw beginnen' vrijwel onmogelijk voor criminelen die met naam en toenaam via internet te boek staan als 'gezocht' (Prins 2009: 119). Het karakter van het internet is er een van bewaren en kopiëren, niet van vergeten. Ook technisch gezien is vergeten niet meer nodig vanwege de beschikbare opslagcapaciteit. Wettelijke regelingen stellen weliswaar een tijdslimiet aan het bewaren van gegevens, maar het opschonen van gegevensbestanden lijkt op uitvoeringsniveau nauwelijks prioriteit te hebben (Neuman & Calland 2007; Buruma 2011). Bovendien is bij veel organisaties en zeker opsporingsinstanties de opvatting leidend dat de gegevens ooit nog hun belang kunnen tonen. Het onderzoek van Choenni et al. (2011) concludeert bijvoorbeeld dat in het landelijke HerKenningsdienst Systeem (HKS)-bestand van

de politie (dat namen van personen bevat tegen wie een proces-verbaal is opgemaakt) 8.000 verdachten staan die in werkelijkheid reeds overleden zijn. Bovendien blijken 2.800 vrijgesproken personen ten onrechte in het systeem voor te komen. Alhoewel het hier in aantallen om relatief kleine percentages van het totaal aantal geregistreerden gaat, concluderen de onderzoekers dat uitgebreider onderzoek naar de mate van vervuiling in politiesystemen noodzakelijk is, zeker nu de politie deze en andere databanken inzet voor het opstellen van risicoprofielen en de systemen steeds vaker aan elkaar worden gekoppeld. Eerder al concludeerde Grijpink dat er in het geautomatiseerde vingerafdrukkensysteem Havank van de Nederlandse politie meer dan 101.000 aantoonbare identiteitsfraudeurs zijn te vinden (Grijpink 2006b).

Box 4.2 Onverwacht geheugen: auto legt rijgedrag automobilist vast

Informatietechnologie is niet gelijk te stellen aan een revolutionaire opslagcapaciteit: daaraan voorafgaand wordt er ook exponentieel meer informatie gegenereerd. Elke sensor, elke chip genereert output. Die output heeft een bepaalde functie, maar kan ook voor een onverwachte nieuwe bestemming worden aangewend. Dit illustreert het geval van het geheugen van de auto. De meeste auto's hebben diagnostische informatiesystemen die met name de prestaties van de motor monitoren. Deze OBD-technologie (On Board Diagnostics) is in Europa sinds 2001 voor de meeste auto's verplicht gesteld, met het oog op de bescherming van het milieu. Dit standaardsysteem registreert de emissie van de motor, waarschuwt zo nodig de bestuurder, en stelt mecaniciens in staat om problemen op te sporen. Verder staat het fabrikanten vrij om slimmere systemen te bouwen, met meer functionaliteiten en daardoor met een rijker geheugen. Zo zijn bepaalde merken auto's voorzien van een zogenaamde Event Data Recorder die gegevens opslaat over een bepaald voorval, bijvoorbeeld welke snelheid een auto had voorafgaand aan het moment van een botsing. Deze gegevens zijn handig voor garages bij onderhoudswerkzaamheden, maar ze blijken ook in andere situaties waardevol. Zo wist de politie met behulp van dit autogeheugen de snelheid te achterhalen van een pickup truck die was betrokken bij een verkeersongeval, eind 2009 in Rotterdam. Daarbij vielen vier doden. De bestuurder van de auto behaalde tot vijf seconden voor het ongeluk een snelheid van 147 kilometer per uur en werd in september 2010, mede op basis van deze informatie voor roekeloos rijgedrag veroordeeld. Voor het uitlezen van de betreffende informatie, waar andere korpsen in Nederland (nog) niet toe in staat zijn, was een stevige dosis technisch vernuft nodig (*NRC Next*, 26 april 2010).

Burgers staan in de praktijk van alledag vrijwel machteloos wanneer ze het foutieve virtuele beeld dat van hen bestaat willen corrigeren. Want nog afgezien van een gebrek aan aandacht bij politie en justitie voor het verwijderen en overschrijven van informatie in systemen, blijkt het voor hen vrijwel onmogelijk om inzicht te krijgen in de gegevens die zoal over hen worden bewaard – het procesmatige beginsel van transparantie. Verzoeken tot kennisname van informatie die nooit in een strafdossier terechtkomt maar wel wordt bewaard (journaals, aantekeningen

van interviews met mensen die niets bruikbaars te vertellen hadden, processen-verbaal van activiteiten die geen resultaat opleverden e.d.), worden vrijwel nimmer gehonoreerd (Kielman 2010: 157; Buruma 2011). Er is wel een wettelijk, maar geen daadwerkelijk en effectief systeem om op de hoogte te worden gebracht van de methoden die tegen een burger zijn ingezet, terwijl er ook geen reëel systeem is waaruit die burger kan vernemen wat er eigenlijk over hem of haar is opgeslagen (Buruma 2011). Ook het recht op verbetering van gegevens blijkt problematisch. Het blijkt zeker geen uitzondering dat iemand die *achteraf* ten onrechte als verdachte blijkt te zijn aangemerkt, bijvoorbeeld als gevolg van (administratieve) fouten van politie of parket, op een zodanige wijze in de systemen gecodeerd blijft dat er een gerede kans is dat er vanuit justitie negatief wordt geadviseerd op zijn aanvraag voor bijvoorbeeld een Verklaring omtrent het gedrag of het verkrijgen van een bepaalde vergunning (Buruma 2011).

4.4 BOUWEN EN BEWIJZEN

Op de bestuursniveaus die in dit gedeelte aan de orde zijn geweest (uitvoeringsorganisaties, agentschappen en decentrale bestuursorganen) moet 'het' veelal gebeuren. Hier worden de applicaties meestal gebouwd – autonoom dan wel als schakel in een landelijk dekkend systeem – en hier moeten systemen zich bewijzen in de interactie met de 'klant', maar ook met de mensen die de uitvoering ter hand nemen. Hetzelfde kan gezegd worden vanuit het perspectief van de beginselen: juist in de concrete uitwerking moeten zij bewezen worden. Daarbij vertegenwoordigt besluitvorming die 'dicht bij de mensen staat' ook een bepaalde waarde. In een uitvoeringsorganisatie kan specifieke expertise tot ontplooiing komen, en bij een gemeente kunnen lokale wensen en omstandigheden in ogenschouw worden genomen. Niettemin kan een grote diversiteit op uitvoeringsniveau de evenwichtige opbouw van de eOverheid ook bedreigen. In het voorgaande waren situaties aan de orde die de indruk wekken dat *anything goes* soms het devies is (cameratoezicht, het voorbeeld van 'Topic View'). Tegelijkertijd werd gesignaleerd dat er een roep is om meer sturing en ondersteuning. Daaruit kan worden afgeleid dat de veelkleurige en soms chaotische aanblik die de eOverheid op uitvoeringsniveau en lokaal geeft, vaak niet moedwillig is nagestreefd.

De stuwende beginselen veiligheid en effectiviteit en efficiëntie zijn ook op uitvoeringsniveau en lokaal dominante motieven. Die beginselen worden vaak terecht als dwingend ervaren. Er gelden wel degelijk technologische imperatieven. De overheid functioneert immers niet in een vacuüm: ICT-innovatie biedt veel kansen die niet zomaar versmaad kunnen worden, en in de maatschappij zijn deze innovaties zodanig ingevoerd dat de overheid zich ook daartoe heeft te verhouden. Een duidelijk voorbeeld van zo'n technologisch-maatschappelijk imperatief is de zorg die de overheid heeft voor de vaststelling van identiteiten. Die is aan de orde bij de hiervoor beschreven behoefte aan een 'hoger niveau van

authenticatie' dan bij de thans beschikbare instrumenten aanwezig is. Identiteitsdocumenten hadden altijd al een belangrijke functie in het maatschappelijk verkeer aangezien niet alleen de overheid, maar ook burgers onderling betrouwbare identificatie verlangen. In het huidige tijdperk is de behoefte aan (veilige) digitale identiteitswaarborgen even groot, om de eenvoudige reden dat de digitale wereld een laag aan het sociale leven heeft toegevoegd. De vraag is dan of de overheid moet voorzien in technologische oplossingen voor de digitale identiteitsproblemen die op dit moment steeds urgenter worden. Dat bijvoorbeeld de RDW met zijn ideeën voor het eRijbewijs de boer op gaat lijkt dan ook gunstig voor de gedachtevorming over deze overheidstaak. Zoals opgemerkt zijn er op dit thema meerdere overheidsorganisaties tegelijk bezig om 'hun' oplossing 'op de kaart' te zetten. Tegelijkertijd is het feit dat verschillende overheden op dit punt een soort entrepreneursrol aannemen een indicatie van een onevenwichtigheid en gebrek aan regie. Er is, zo blijkt uit talloze voorbeelden, enorm veel ruimte voor de ambities van publieke actoren, maar ook voor die van private actoren die een graantje mee willen pikken. Dit vrije speelveld wordt door betrekkelijk weinig kaders omsloten.

Het ontstaan van Veiligheidshuizen is illustratief voor deze vrijheid. Dit is een belangwekkende en voor burgers ingrijpende ontwikkeling: het zijn knooppunten voor hoogst sensitieve informatie uit allerlei bronnen. Niettemin zijn Veiligheidshuizen op lokaal niveau spontaan opgekomen (Holvast & Bonthuis 2010) en moeten zij het nog steeds zonder speciale spelregels stellen. Deze Veiligheidshuizen zijn niet de enige voorbeelden van ontwikkelingen die gekenmerkt worden door een sterke diversificatie van actoren, die worden uitgenodigd 'in de keuken' van domeinen waar zij tot dusver niets mee te maken hadden. De ad hoc en daardoor lang niet altijd doordacht tot stand gekomen rolverdelingen, en het veelal ontbreken van kaders, zorgen voor veel onduidelijkheid. Die onduidelijkheid komt de effectiviteit en efficiëntie van het beleid – waar het allemaal om begonnen was – niet ten goede. ICT-systemen komen niet zelden in zwaar weer terecht: situaties waarin de belofte om het bestaande beter (efficiënter, effectiever) te doen, niet bewaarheid wordt. Door een instrumentele lens wil nogal eens het besef van de enormiteit van sommige ambities vertroebelen, zoals werd opgemerkt ten aanzien van het Antwoord©-initiatief, dat het summum van maatwerk in het vooruitzicht stelt. Het is geen sinecure om een systeem te ontwikkelen en te onderhouden dat voldoet aan de hooggestemde verwachtingen, ook in de wijze waarop de *street level bureaucrat* ermee werkt. Zoals hiervoor op diverse plaatsen is opgemerkt, is er bij de totstandkoming van de applicaties van de eOverheid vaak sprake van 'Babylonische' communicatiestoornissen tussen bestuurders en ontwikkelaars, of tussen beleidsmakers en uitvoerders. Ook doen de inherente technologische risico's van interpretatiefouten bij data mining en anderszins onleesbare archieven zich voor, zonder dat deze problemen tot een echte herbezinning leiden op de ICT-systemen en hun interactie met de gebruiker. Ook systemen

kunnen aan communicatieproblemen lijden, en doen dat vaak ook, getuige de hoge prioriteit die aan interoperabiliteit en semantische stroomlijning gegeven wordt. Verder maakt de ontwikkeling van de eOverheid op lokaal niveau ook duidelijk dat aan decentralisatie een prijskaartje hangt, en dat het eigenlijk niet efficiënt en effectief is om (te) kleine gemeenten verantwoordelijk te maken voor de 'uitrol' van het hele scala aan applicaties. Daar komt bij dat de eOverheid nog een heel stuk duurder zou zijn als er op alle niveaus sprake was van verantwoorde zorg voor de kwaliteit van informatie. Het voorbeeld van de Belastingdienst die zich genoodzaakt ziet om een parallel persoonsregistratiesysteem in de lucht te houden, omdat de GBA, het beoogd universele systeem, niet voldoende accuraat is, spreekt in dit opzicht boekdelen.

Er wordt aanmerkelijk minder gebouwd aan de verankerende en procesmatige beginselen, en er is enige schroom om die beginselen zich te laten bewijzen. De meest markante ontwikkeling, die meermalen aan bod is gekomen, is de erosie van schotten tussen beleidsterreinen en tussen overheidsorganisaties op uitvoerings- en lokaal niveau, ook in relatie tot de private sector. Deze schotten worden in toenemende mate – ook in de publieke opinie – als beletselen gezien, voor daadkracht, maar ook voor herkenbaarheid. De overheid die één gezicht heeft, en die zich bij één loket laat benaderen, is niet een overheid die intern heel streng is opgedeeld. Maar met de vooruitgang die ontschotting ten behoeve van herkenbaarheid (de één-loket-gedachte) en ontschotting ten behoeve van daadkracht (werken in ketens en netwerken) hebben geboekt, gaat er ook iets verloren. Witteveen (2010: 219) karakteriseert het weberiaanse ideaal als volgt: "De opkomst van de bureaucratie vindt plaats in liberale samenlevingen die vrijheid nastreven door domeinen van elkaar te scheiden." Schotten functioneren – met al hun nadelen – als een middel om zorgvuldig en afgebakend overheidshandelen te bevorderen, en daarmee om de vrijheid van burgers te beschermen. De burger kan zich autonoom ontwikkelen, oftewel zijn keuzevrijheid en privacy koesteren, waar hij weet dat overheidsorganisaties met een specifieke focus zijn opgericht, en buiten hun nauw omschreven taken en bevoegdheden geen activiteiten mogen ontplooien, hoe wenselijk die activiteiten anderszins ook mogen zijn. Die focus van overheden wordt op het informationele vlak steeds onscherper – getuige ook het ontstaan van 'virtuele organisaties' zoals RINIS – waardoor burgers er rekening mee moeten houden dat 'hun' informatie in publieke handen een eigen leven kan gaan leiden. Terwijl de belangen en doelstellingen van overheidsorganen onderling zeer verschillend kunnen zijn en behoren te zijn – zoals het verschil van inzicht tussen de politie en de gemeente bij uitgifte van vervangingen voor gestolen paspoorten bijvoorbeeld laat zien – maken deze overheden toch steeds vaker gebruik van dezelfde 'gepoolde' informatie.

4.5 CONCLUSIE

De eOverheid heeft al met al veel barrières geslecht, maar nog geen begin van een idee ontwikkeld over de bredere en meer fundamentele consequenties van een gedigitaliseerd en ontschot uitvoeringsniveau. In het bijzonder raakt deze leemte de positie en de bescherming van burgers. Vaak is sprake van een asymmetrie tussen wat de uitvoeringsinstanties, gemeenten en politie door ICT 'zijn gaan kunnen', en wat zij ondernomen hebben om de burger in staat te stellen met de digitale ontwikkeling mee te groeien. In plaats van een symmetrische *empowerment* van de burger is eerder te zien dat er steeds meer alertheid en vaardigheid van burgers wordt gevraagd, omdat hun inzicht en bewijspositie erop achteruit is gegaan. Ook het werken in ketens en netwerken gaat niet gepaard met een herbezinning op verantwoordelijkheden, in het licht van de positie van de burger. Dat levert een speelveld op van creatief en veelal met goede bedoelingen opererende overheden, maar met weinig structureel houvast voor burgers. Er zijn wat betreft de relatie overheid-burger(s) nog geen nieuwe lijnen zichtbaar in de nieuwe door ICT gecreëerde uitvoeringsrealiteit. Het speelveld verandert elke dag, en ogenschijnlijk vanzelf, maar van een institutionele herbezinning is geen sprake. Als echter de aandacht uitsluitend naar het speelveld blijft uitgaan en niet naar de beschermende kaders, zal de sluipende verzwakking van de positie van de burger doorgaan.

Een urgent aspect in dit verband betreft het ontbreken van een visie op en kaders voor 'vergeten'. Als de opmars van ICT immers iets heeft duidelijk gemaakt is het dat vergeten niet meer vanzelf gaat. Het langzaam dagende besef dat vergeten een deugd is (Mayer-Schönberger 2009) heeft enerzijds te maken met de constatering dat het nogal eens schort aan de kwaliteit van overheidsinformatie en houdt anderzijds verband met het verslechteren van de privacypositie van burgers: als niets meer verdwijnt kan het individu ook nergens meer van los komen. Ook niet van het beeld dat de overheid met behulp van technologie en informatie over en van hem heeft gecreëerd. Deze 'beelden uit het verleden', die vanwege de technologie veel krachtiger doorwerken in het heden, hebben de neiging om burgers vast te pinnen op een bepaalde (veronderstelde) identiteit, waardoor de autonomie (keuzevrijheid) van die burgers als het ware 'onderhuids' wordt ingeperkt. Hier gebeurt hetzelfde als bij de 'beelden van de toekomst', die door profilering worden geconstrueerd op basis van beelden van het verleden en heden. Er zal kortom vanuit het besef dat vergeten een belang dient (overigens niet alleen van burgers maar ook van de overheid) moeten worden gebouwd aan de verankerende en procesmatige kaders voor de eOverheid.

Ten slotte, de op dit moment nogal achterstallige transparantie en accountability van de uitvoeringspoot van de eOverheid kan eigenlijk alleen door de (centrale) overheid zelf worden rechtgetrokken, want zonder nadere ondersteuning en faci-

litering kan een individuele burger niet tot de binnenste cirkel van de informatiehuishouding van de overheid doordringen. De door ICT ondersteunde assertieve burger kan veel *beleids*informatie loskrijgen en verspreiden, of zelfs genante beleidsinformatie en andere overheidsgerelateerde informatie verspreiden (zie WikiLeaks) dan wel genereren (zie hoofdstuk 7). Maar deze zelfde assertieve burger staat ten aanzien van de informatie die zijn *individu* aangaat – de grondstof van de besluiten en beschikkingen van de eOverheid – dikwijls beduidend zwakker. De kaders voor de informatiepositie (transparantie) van burgers en de ingangen (accountability) voor burgers ontstaan niet vanzelf.

NOTEN

1 Richtlijn 2006/126/EG van het Europees Parlement en de Raad betreffende het rijbewijs, *Pb* L [2006] 403, blz. 18-60.

2 Bij authenticatie gaat het om het aantonen (met behulp van onder meer digitale technieken) dat iemand is wie hij zegt te zijn.

3 De Belastingdienst, Centraal Bureau voor de Statistiek (CBS), Centraal Justitieel Incassobureau (CJIB), College voor Zorgverzekeringen (CVZ), Informatie Beheer Groep (IB-Groep), Immigratie- en Naturalisatiedienst (IND), Kadaster, Kamers van Koophandel (KvK), RDW, Sociale Verzekeringsbank (SVB), UWV.

4 Gesprek met dhr. A. Zuurmond, oprichter en partner Zenc; hoogleraar TU Delft; oktober 2010.

5 Een sector bestaat uit een of meerdere organisaties, bij meerdere organisaties wordt gewerkt met een loket: het Sectoraal Aanspreekpunt (SA). Een SA zorgt ervoor dat gegevens op de juiste plek worden aangeboden of opgehaald binnen de sector.

6 http://www.ocwduo.nl/klantenservice/privacy/privacy.asp.

7 Gesprek met de Eerste Kamerleden R.H. van de Beeten, H. Franken, J. Hamel, P.L. Meurs, I.Y. Tan, C.P. Thissen, mei 2010.

8 NRC *Handelsblad*, april 2010.

9 Een verwijsindex is een ICT-toepassing waarin meldingen ofwel signalen worden opgenomen en uitgewisseld. Met name in de (jeugd)zorg wordt dit instrument gebruikt om contact tussen verschillende hulpverleners mogelijk te maken. Voor een overzicht: CapGemini Consulting (2010b).

10 Een koppelvlak is een geheel van gemeenschappelijke afspraken om de uitwisseling van elektronische berichten tussen twee of meer ketenpartners mogelijk te maken.

11 Een landelijk schakelpunt is een centraal knooppunt voor de landelijke uitwisseling van gegevens (bijvoorbeeld patiëntgegevens) tussen lokale actoren (bijvoorbeeld zorgaanbieders).

12 MEE bundelt organisaties ter ondersteuning van individuen die leven met een handicap: http:// www.mee.nl.

13 “Na inventarisatie blijkt dat ruim 300 cliëntgegevens door twee of meer van de betrokken indicatieorganisaties worden gebruikt. Uit onderzoek blijkt dat een deel van deze gegevens al kan worden uitgewisseld. Voor het andere deel is dat juridisch nog niet mogelijk. Om de wettelijke belemmeringen weg te nemen, wordt het project Indicatiedossier voortgezet als (wetgevings)traject Gegevensuitwisseling, gecoördineerd door het ministerie van SZW. Doel is om een optimale gegevensuitwisseling tussen de organisaties mogelijk te maken” (Ministerie van SZW & Ministerie van VWS 2010: 7).

14 Het stelsel bestond in 2010 uit dertien basisregistraties met gegevens over personen, bedrijven, gebouwen, adressen, geografie/kaarten, percelen, voertuigen en

inkomens: Gemeentelijke Basisadministratie persoonsgegevens (GBA), Nieuwe Handelsregister (NHR), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Topografie (BRT), Basisregistratie Kadaster (BRK), Basisregistratie Voertuigen (BRV), Basisregistratie lonen, arbeids- en uitkeringsverhoudingen (BLAU), Basisregistratie Inkomens (BRI), Basisregistratie onroerende Zaken (WOZ), Registratie Niet Ingezetenen (RNI), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Bodem en Ondergrond (BRO).

15 www.e-overheid.nl.

16 Bij semantische interoperabiliteit wordt de context waarin de gegevens worden gebruikt van belang en daarmee wordt ook geaccepteerd dat er variatie in de betekenis van deze gegevens kan zijn. Zie onder meer Wisse 2008.

17 De 10 in 2005 door het programma Burger@Overheid.nl geformuleerde criteria (Burger@Overheid.nl 2006) zijn: keuzevrijheid contactkanaal; vindbare overheidsproducten; begrijpelijke voorzieningen; persoonlijke informatieservice; gemakkelijke dienstverlening; transparantie werkwijzen; digitale betrouwbaarheid; ontvankelijk bestuur; verantwoordelijk beheer; actieve betrokkenheid.

18 Interview met dhr. J. Hakkenberg, directeur Rijksdienst voor het Wegverkeer, lid ICTU stichtingsbestuur, voorzitter van de Manifestgroep, mei 2010.

19 Gesprek met dhr. H. Tankink, waarnemend directeur Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) en dhr. J.W. van Dongen, Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR), november 2009.

20 Kamerstukken II, 2009/10, 29 362, 157 presenteert in optimistische toon een diversiteit aan projecten, diverse daarvan vallen onder het Nationaal Uitvoeringsprogramma Dienstverlening en e-Overheid – NUP.

21 Gesprek dhr. H. Gardeniers en dhr. E. Schreuders, Net2Legal, februari 2010.

22 Interview met dhr. H. van Duivenboden, b&a Consulting/hoogleraar informatisering en interbestuurlijke samenwerking Universiteit van Tilburg, mei 2010.

23 Interview met dhr. J. Hakkenberg, directeur Rijksdienst voor het Wegverkeer, lid ICTU stichtingsbestuur, voorzitter van de Manifestgroep, mei 2010.

24 http://www.e-overheidvoorburgers.nl/producten,antwoord.

25 Nodale oriëntatie is een wijze van opereren waarbij de politie expliciete aandacht heeft voor stromen van mensen, goederen, geld en informatie. De knooppunten (nodes) van de infrastructuur van deze stromen worden als aangrijpingspunt voor het handelen van de politie genomen. Zie http://www.politie.nl/overdepolitie/Politie_in_ontwikkeling/Visie/Nodale_orientatie.asp.

26 Het idee om met camera's iedereen op de toegangswegen tot steden te volgen met de bedoeling kwaadwillenden te signaleren en tegen te kunnen houden, wordt in de wandelgangen de 'virtuele slotgracht' genoemd.

27 Interview met het Radio1 Journaal op 9 september 2010.

28 http://23opsporingsdingen.nl (geraadpleegd op 24 september 2010).

29 http://www.forensischinstituut.nl/producten_en_diensten/producten/kecida.aspx (geraadpleegd op 24 september 2010).

30 Een website voor politiemensen stelt hierover: "Juridisch gezien geldt voor internet eigenlijk hetzelfde als het echte leven."(http://230psporingsdingen.nl, geraadpleegd op 24 september 2010).

31 De jurisprudentie laat een wisselend beeld zien. Zie: NRC *Handelsblad*, 19 oktober 2010, blz. 2 met toelichting van Ybo Buruma (NRC/NJblog uitspraak 19 oktober 2010).

32 *Algemeen Dagblad*, 8 december 2010.

5 SCHAALVERGROTING ZONDER GRENZEN

Het opzetten van informatiesystemen en het maken van koppelingen daartussen is inmiddels zo ongeveer de *lingua franca* van modern mondiaal besturen. Het spreekt daarom voor zich dat informatiestromen zich niet tot de landsgrenzen laten inperken. Terwijl informatietechnologie van zichzelf al territoriale afgrenzingen relativeert – zoals de WRR in 1998 constateerde – is die karakteristiek tegenwoordig ook enthousiast omarmd door overheden. De wereldwijde *security drive* na de aanslagen van 11 september 2001 is hier bepalend voor, maar ook de mate waarin de lidstaten van de EU op allerlei beleidsterreinen met elkaar verweven zijn geraakt. Het uitwisselen van informatie is immers niet alleen voor veiligheidsdiensten van belang, het is binnen Europa tevens bevorderlijk voor de verdere vervolmaking van de interne markt en voor de effectiviteit van allerhande vormen van bestuurlijke samenwerking. Alhoewel Nederland op bilateraal niveau initiatieven ontplooit en afspraken maakt over het uitwisselen van gegevens (zoals eind 2010 met de Verenigde Staten over het verschaffen van toegang tot elkaars databanken ten behoeve van *matching* van vingerafdrukken en DNA-profielen[1]), wordt de inzet van technologie en de uitbouw van informatiestromen primair bepaald door ontwikkelingen op Europees niveau. Inmiddels is er sprake van een groeiend aantal Europese databanken waarin persoonsinformatie 'grenzeloos' rondgaat, en op basis waarvan bestuursorganen in EU-lidstaten besluiten nemen. De reikwijdte van deze databanken is groeiende. Dergelijke Europese systemen markeren een hoge mate van integratie: ook de Europese overheid laat zich nadrukkelijk als een eOverheid zien. Maar daarnaast is de EU ook een bron van wetgeving die voor de nationale eOverheden maatgevend is. Het privacyrecht is bijvoorbeeld grotendeels Europees ingevuld.

De Europese applicaties en de Europese regulering van de eOverheid hebben herkenbare karaktertrekken, maar vinden plaats in een totaal andere institutionele setting. In het onderstaande zullen de databanken worden geanalyseerd in het licht van de rol en positie van de actoren op dit toneel. Dit zijn niet alleen de instellingen van de EU, maar een divers gezelschap van actoren en gremia die inwerken op de Europese beleidsvorming.

5.1 EUROPESE INFORMATIEBESTANDEN EN -STROMEN

"Het Schengengebied en de interne markt zouden niet kunnen functioneren zonder grensoverschrijdende informatie-uitwisseling", zo opent de Europese Commissie het halverwege juli 2010 gepubliceerde document met daarin "voor het eerst een volledig overzicht (…) van alle EU-maatregelen op het gebied van de verzameling, de opslag en de grensoverschrijdende uitwisseling van persoonsgegevens met het oog op rechtshandhaving en migratiebeheer die al zijn ingevoerd,

die nu worden ingevoerd of waarover wordt gesproken" (Europese Commissie 2010a: 2, 31). Opvallend in het betoog van de Commissie is dat de crux van de ontwikkelingen primair op het niveau van de informatie zit en veel minder op dat van de technologie. De in het document gepresenteerde beleidsstrategie richt zich op informatie en doet een voorzet voor de discussie over "de vraag of er een Europees model voor informatie-uitwisseling moet komen op basis van een evaluatie van de bestaande informatie-uitwisselingsmechanismen" (Europese Commissie 2010a: 3). Natuurlijk doen innovaties in het domein van de hardware (opslagcapaciteit, rekencapaciteit en de snelheid en draagbaarheid van applicaties), in software (interactiviteit, web 2.0) en andere technische faciliteiten (biometrie, RFID) er in het Europese beleid toe. Maar de implicaties van europeanisering, globalisering en schaalvergroting tonen zich toch primair bij de grensoverschrijdende informatiestromen. De tientallen databanken die de afgelopen jaren op Europees initiatief van de grond kwamen, verbinden Nederlandse burgers en hun gegevens op virtuele wijze met de miljoenen burgers in andere lidstaten. De ruimhartige mogelijkheden tot (al dan niet rechtstreeks) gebruik van deze databanken door de lidstaten en de VS zijn neergelegd in een scala aan formele regels gecomplementeerd met een – ook voor het Europees Parlement[2] – onbekend aantal schimmige bilaterale en informele afspraken. Zowel de tekst van de genoemde Mededeling van de Europese Commissie als de bijlagen roepen het beeld op van een grenzeloos versmolten digitale grabbelton, waarbij ons land overigens tot de grootverbruikers kan worden gerekend (zie bijv. Broeders 2009). Toch blijkt op cruciale momenten ook dat van grensoverschrijdende gegevensuitwisseling juist geen sprake is, zoals bij de Amsterdamse zedenzaak in december 2010. De hoofdverdachte bleek al eerder in Duitsland veroordeeld voor bezit van kinderpornografie. Maar omdat het Europees informatiesysteem over strafbladen (ECRIS) waartoe al in 2007 werd besloten, zich eind 2010 nog steeds in een testfase bevond, was zijn strafblad niet bekend bij de Nederlandse autoriteiten. Desalniettemin, het beeld dat uit de empirie van de Nederlandse situatie oprijst, beperkt zich niet tot de landsgrenzen. Meer en meer zorgen processen van globalisering ervoor dat het informatiebeleid van de Nederlandse overheid op een hoger schaalniveau wordt gedicteerd en georganiseerd, en bovendien in internationale (Europese) applicaties en systemen wordt uitgewerkt.

5.1.1 INTERNATIONALE VEILIGHEID ALS MOTOR

De belangrijkste motoren achter de internationalisering van informatiestromen zijn de systemen die zijn ingericht voor de aanpak van illegale migratie en grensoverschrijdende criminaliteit en in het bijzonder in de strijd tegen het internationale terrorisme die de VS hebben ingezet en aangevoerd na de aanslagen op New York en Washington in 2001. Nationale veiligheid, en de vermenging van immigratie met veiligheidsvraagstukken zijn belangrijke drijvende krachten achter deze nieuwe digitale informatiestromen (Lyon 2003; Zureik & Salter 2005; Boswell 2007; Guild 2009). Ook, of misschien wel juist, in Europa is bij politici en beleids-

makers het technovertrouwen en het enthousiasme voor het digitaal uitwisselen van informatie als oplossing voor deze problemen groot. Het Europees Parlementslid Coelho waarschuwde in deze context enkele jaren geleden al voor "an atmosphere of the 'impossibility of error' under all circumstances" waar burgers de dupe van kunnen worden (Liberatore 2005: 15).

Box 5.1 De techniek wijst de weg: Europese migratiedatabanken

In de afgelopen twintig jaar is op Europees niveau een netwerk van databanken ontwikkeld en ingevoerd om migratie 'beheersbaar' te maken. De verleiding van nieuwe technologische mogelijkheden bleek daarbij groot: geen van de systemen is beperkt gehouden tot het doel waarvoor het oorspronkelijk werd opgericht. De geschiedenis van de migratiedatabanken laat bovenal zien dat bij de keuzes over de technologie bewust is voorgesorteerd op deze latere uitbreidingen en toevoegingen.

Het Schengen Informatie Systeem (SIS) was al snel zo populair dat al in 1996 werd besloten een SIS II-systeem te ontwikkelen. De ontwikkelingsfase loopt echter nog steeds en gaandeweg legden de lidstaten steeds weer nieuwe wensen op tafel. In hoofdzaak ging het daarbij om het toevoegen van meer informatiecategorieën, met name biometrie, en om de toegang tot de gegevens van nieuwe organisaties, met name criminaliteits- en terrorismebestrijders. De Europese Commissie heeft zich pragmatisch opgesteld tegenover deze verlanglijstjes: in afwachting van de uitkomst van de politieke besluitvorming lieten ze een systeem ontwikkelen dat al aan deze wensen voldeed. Het systeem "must be designed and prepared for biometric identification to be implemented easily at a later stage, once the legal basis, allowing for the activation of such potential functionalities, has been defined" (Europese Commissie 2003: 16). Het in 2007 genomen politieke besluit over de functies van SIS II noemt vingerafdrukken en foto's, maar een onderzoeksrapport van de Britse House of Lords stelt dat het systeem ook geschikt zal zijn voor irisscans en DNA. Technisch kan het, nodig is 'slechts' de creatie van wettelijke ruimte (House of Lords 2007: 20, n. 43). Een vergelijkbare uitbreiding van functies zien we bij Eurodac. Oorspronkelijk opgezet om 'asielshoppen' tegen te gaan, maar al snel aangevuld met doelstellingen om illegale migranten te identificeren. De functie om illegalen te 'checken' en identificeren was optioneel voor de lidstaten, maar al snel zo populair dat de Commissie in haar evaluatie van het systeem voorstelde om voortaan ook de data over illegale immigranten op te slaan, in plaats van alleen te controleren.

Function creep speelt niet alleen binnen het ontwikkelingstraject van een specifiek systeem, maar ook bij verbindingen tussen systemen. Het Visa Informatie Systeem (VIS) wordt ontwikkeld met interoperabiliteit en synergie met de reeds bestaande of in ontwikkeling zijnde systemen als centraal aandachtspunt. VIS en SIS II vormen (nu nog) 'aparte containers', maar de database, de technische lay-out en zelfs de fysieke locatie voor de centrale database zijn hetzelfde. De technische inrichting is volledig geschikt voor koppeling van de databases, waarmee verschillende informatiestromen met elkaar in contact zouden komen.

Zie voor een uitgebreide beschrijving van deze systemen Broeders (2011).

De invloed van Europa doet zich langs twee lijnen gelden. Allereerst is het eigen informatiebeleid van de Nederlandse overheid de afgelopen jaren via diverse Europese maatregelen gestuurd en zeker op het terrein van veiligheid ook gedicteerd. Aangezien Nederland uiteraard een plaats aan de Europese onderhandelingstafel heeft, komen die 'dictaten' minder van boven dan politici het soms doen voorkomen. Sprekende voorbeelden zijn hier de toepassing van biometrie op het paspoort en de dataretentie (het bewaren van gegevens over telefoon- en internetverkeer). De tweede lijn loopt via de ontwikkeling en uitbouw van internationale (Europese) applicaties en systemen. Hier zijn de informatiestromen uiteindelijk eerder Europees dan nationaal van aard en zijn daarmee veelal ook op dat niveau besproken en vastgelegd. Kenmerkende voorbeelden zijn de talrijke migratiedatabanken (Broeders 2007; Balzacq 2008; Dijstelbloem & Meijer 2009; Besters 2010; Besters & Brom 2010). Al sinds 1995 wordt op Europees niveau gewerkt aan een netwerk van databanken die verschillende doelstellingen van het migratiebeleid moeten (gaan) ondersteunen. Leidend zijn hier het Schengen Informatie Systeem (SIS) voor de registratie en opsporing van illegalen en het gebruik van valse en vermiste identiteitsdocumenten, het Eurodac-systeem dat de vingerafdrukken van alle asielzoekers in de EU registreert, met als doel om 'asielshoppen' tegen te gaan en asielverzoeken in het eerste land van aankomst af te handelen (het 'Dublin-systeem') en het Visa Informatie Systeem (VIS) dat binnen enkele jaren van start moet gaan en van alle aanvragers van een EU-visum de persoonsgegevens en de vingerafdrukken in een centrale databank zal vastleggen. Overigens impliceert de uitbouw van Europese systemen nog niet dat de aangesloten landen op een uniforme en eenduidige wijze met de aan te leveren gegevens omgaan. Bij zowel het SIS als Europol blijkt het ene land bepaalde gegevens wel in het register op te nemen, terwijl het andere land dat niet doet.[3]

5.1.2 HET DIGITALE EUROPA

Maar het digitale Europa krijgt ook op andere beleidsdomeinen dan veiligheid, criminaliteitsbestrijding en opsporing vorm. Zo vereisen de doelstellingen van de interne markt en het vrije verkeer van diensten, personen en goederen in toenemende mate een informatie-infrastructuur die dat ondersteunt. Ter uitvoering van de Dienstenrichtlijn[4] is een grensoverschrijdend elektronisch systeem opgezet, het Internal Market Information (IMI)-system, waarmee gegevens voor zowel dienstverlening als controle soepel tussen lidstaten kunnen worden uitgewisseld.[5] De Europese Commissie meldde op 3 augustus 2010 trots met een videoclip dat de 5.000ste instantie toegang tot het systeem was verleend.

Al in de jaren tachtig en in het bijzonder de jaren negentig toonde de Europese Commissie zich actief op het terrein van eGovernment (Kroon & Bekkers 1994). Startpunt vormde het zogeheten Witboek van Delors uit 1993, waarin het belang en de urgentie voor een pan-Europese informatie-infrastructuur voor economi-

sche groei en competitiviteit werd benadrukt (Gomez-Barrosso et al. 2008). In 1999 werd als onderdeel van de Lissabon-strategie, die erop gericht was voor 2010 de Europese Unie de meest competitieve en dynamische kenniseconomie in de wereld te maken, het *eEurope - An Information Society for all*-programma gelanceerd (Europese Commissie 1999). Het programma heeft als voornaamste doelen: "bringing every citizen, home and school, every business and administration into the digital age and online; creating a digitally literate Europe, supported by an entrepreneurial culture to finance and develop new ideas; ensuring the whole process is socially inclusive, builds consumer trust and strengthens social cohesion" (Europese Commissie 1999: 2). Om deze doelen te realiseren zou gewerkt moeten worden aan het creëren van een gunstige juridische context en het ondersteunen van nieuwe infrastructuur. Het vervolgprogramma eEurope 2005 ambieert een verdere vertaalslag naar hogere economische productiviteit en betere en meer toegankelijke diensten voor alle Europese burgers (Europese Commissie 2002). Het i2010-programma vervolgens, promoot een open en competitieve digitale economie en benadrukt de rol van ICT als een drijvende kracht voor (sociale) insluiting en kwaliteit van leven, en legt daarnaast prioriteit bij een grenzeloze Europese informatieruimte en het stimuleren van innovatie (Gomez-Barrosso et al. 2008). Voor een deel van de intra-Europese gegevensuitwisseling, met name als het gaat om diensten voor burgers en bedrijven, geldt daarbij dat het in de praktijk van alledag niet de centrale overheden of de Europese Commissie zijn die het voortouw nemen, maar de nationale (semi)overheidsorganisaties die zich in netwerken van nationale collega-instellingen organiseren om uitwisseling van informatie ter hand te nemen. Met name zelfstandige bestuursorganen (ZBO's) en agentschappen, als de RDW en het Kadaster, zijn daarin actief. 'Europa' faciliteert deze initiatieven, maar deze nieuwe informatiestromen en diensten ontwikkelen zich grotendeels buiten het blikveld van de nationale en Europese publieke opinie. Deze tastbare vorm van Europese integratie voor burgers ontwikkelt zich daarmee op zijn best in de marge van het Europese bewustzijn.[6] De uitzondering op de constatering dat op het terrein van care en service de meerderheid van de ontwikkelingen *bottom-up* tot stand komt, zijn de voorzichtige stappen die de Europese Commissie zet om te komen tot de uitbouw van een Europese infrastructuur voor identiteitsmanagement (Stevens, Elliott, Hoikkanen, Maghiros & Lusoli 2010).

5.1.3 UITBREIDENDE BEWEGINGEN

Wie de vele Europese initiatieven beziet, constateert dat evenals in ons land, ook hier de ontwikkeling wordt gekenmerkt door een continue druk om de functies van de systemen uit te breiden, meer informatiecategorieën toe te voegen en om meer autoriteiten toegang te verlenen tot de opgeslagen data. Dat geldt in mindere mate voor de systemen op het terrein van care en service (alhoewel de Europese Commissie op de website van het hiervoor genoemde Internal Market Information System opmerkt "The Commission is currently exploring with Member States in

which other areas IMI can be used"), maar zeker voor de systemen die zijn geïnitieerd op het Justitie en Binnenlandse Zaken (JBZ)-terrein. Waar bijvoorbeeld de eerste generatie van databanken (SIS, Eurodac en VIS) zich nog in hoofdzaak richt op 'problematische' groepen migranten, zoals asielzoekers en visumplichtige migranten met een risico op illegaliteit, geldt voor de tweede generatie Europese informatiesystemen dat het net veel wijder wordt uitgeworpen (Broeders 2011). Deze tweede generatie richt zich (1) op alle reizende burgers van de wereld en (2) controleert identiteit van alle reizigers met biometrische gegevens waar mogelijk (Broeders 2011; Hampshire & Broeders 2010). PNR-data gaan over alle reizigers, het Europese biometrische paspoort wordt voor alle reizende EU-burgers uitgerold, hoewel er verschillen zijn tussen de lidstaten in de mate waarin de gegevens ook centraal worden opgeslagen (Böhre 2010). Op de Europese tekentafel ligt bovendien een voorstel voor een EU-breed Entry/Exit-systeem dat, naar model van het Amerikaanse US-Visit systeem, de biometrische gegevens van alle in- en uitreizende personen moet gaan registreren (Koslowski 2008; Hobbing & Koslowski 2009). Hoewel dit voornemen nog geen juridische basis heeft, blijft het in alle sleuteldocumenten van de Commissie en de Raad terugkomen en maken conferenties en haalbaarheidsstudies in Brussel de geesten rijp voor de volgende slag in de digitalisering van het Europese migratiebeleid.

De uitbreidende bewegingen tonen zich niet alleen in een stapeling van functies, maar ook in een aangroeiend palet van actoren. Niet alleen in ons land, maar ook op Europees niveau is er veel aandacht vanuit beleid en politiek voor de gegevensverzamelingen die in de private sector worden aangelegd. En ook hier worden de grenzen tussen publiek en privaat daarmee diffuser: bankgegevens worden uit het private bankennetwerk Society for Worldwide Interbank Financial Telecommunication (SWIFT) gehaald, luchtvaartmaatschappijen leveren de zogenaamde Passenger Name Records (PNR data) aan de autoriteiten van de Verenigde Staten, Canada en Australië (Mitsilegas 2009; De Hert & De Schutter 2008; Tweede Kamer 2010-2011e: 2). Aan een meer omvattende EU-regeling voor de verstrekking van PNR-gegevens van passagiers die reizen tussen de Europese Unie en alle derdelanden wordt inmiddels gewerkt (Europese Commissie 2010a: 20; Tweede Kamer 2010-2011e, 2-5). En ondertussen geraakten de EU en VS eind december 2010 wederom met elkaar in conflict over de exacte reikwijdte van de afspraken over het uitwisselen van zowel de bank- als passagiersgegevens.[7] Een ander voorbeeld van de belangstelling die de overheid aan de dag legt voor gegevensverzamelingen van de private sector is de dataretentie-richtlijn. Deze maatregel, geïnitieerd na de aanslagen in Londen in juli 2005, verplicht internet- en telecommunicatiebedrijven om de verkeersgegevens van hun klanten voor langere tijd op te slaan en beschikbaar te houden voor de overheid.[8]

De uitbreidende beweging kent nog een laatste dimensie, namelijk daar waar nationale overheden de nieuwe Europese initiatieven benutten om nog een

stap(je) verder te zetten. Een voorbeeld hiervan is de Europese regeling voor de toepassing van biometrie op het paspoort, die tot doel had de grensoverschrijdende fraude met paspoorten aan te pakken. Nederland benutte de implementatie van de Europese regeling echter ook om een nationale databank met biometrische gegevens te realiseren die mede voor opsporingsdoeleinden gebruikt kan worden (Böhre 2010; Hermans 2010), zoals de RDW de rijbewijzenrichtlijn wil benutten om van het rijbewijs een elektronisch identificatie-instrument te maken. Wat verder in het verleden ligt het traject rondom de Wet vorderen gegevens. Deze wet, die in 2006 in werking trad, vloeit voort uit in oktober 2001 tot stand gekomen Europese afspraken die tot doel hadden de wederzijdse rechtshulp tussen lidstaten te verbeteren met het oog op de bestrijding van georganiseerde en financiële criminaliteit, in het bijzonder witwassen.[9] Het protocol werd na de aanslagen in New York versneld aangenomen en bevatte in de uiteindelijke versie onder meer de bevoegdheid voor justitiële autoriteiten om bij financiële instellingen gegevens te vorderen. Tot die tijd konden banken zelf beslissen of ze de gegevens al dan niet verstrekten (MacGillavry 2000). In ons land benutte de regering de Europese regeling als vehikel om een groot aantal vergaande voorstellen van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij mee te nemen (commissie-Mevis 2001). Met als eindresultaat dat de wettelijke maatregelen zich in ons land niet beperken tot financiële criminaliteit, maar ieder misdrijf. Bovendien zijn de maatregelen vergaand: in het belang van het onderzoek kan een opsporingsambtenaar ook allerhande identificerende gegevens van niet-verdachte personen vorderen. En in bepaalde situaties is het bovendien toegestaan 'toekomstige gegevens' te vorderen, dat wil zeggen dat gegevens die in een komende periode van vier weken ontstaan aan justitie dienen te worden doorgegeven, waarbij dat soms ook '*real-time* gegevens' kunnen zijn.

5.1.4 HAPERENDE DEMOCRATISCHE CONTROLE

De Europese Toezichthouder voor Gegevensbescherming heeft keer op keer gewaarschuwd voor de bijna natuurlijke neiging tot uitbreiding en stapeling, de neiging om vraagstukken en daarmee beleidsterreinen van veiligheid met migratie te vermengen en de neiging om de betrouwbaarheid van technologie, in het bijzonder biometrie, te overschatten (EDPS 2006). Ook het Europees Parlement heeft zich keer op keer kritisch betoond op de informatieverzameling en uitwisseling op het JBZ-terrein, maar had tot de inwerkingtreding van het Verdrag van Lissabon niet de formele bevoegdheid van democratische controle. De Raad van Ministers nam in de regel 'kennis van' de bezwaren van het Europees Parlement zonder iets aan de voorliggende voorstellen te veranderen.

De nationale parlementen, waar de democratische controle tot voor kort wel was belegd, ontbrak het in de regel aan inzicht in de inhoud van de voorstellen en de timing van het Brusselse beleidsproces. Zo hebben de parlementen van de lidsta-

ten nauwelijks invloed gehad op de ontwikkeling van deze JBZ-databanken. Het internationale traject van het biometrisch paspoort in de ICAO, de onderhandelingen met de VS en de besluitvorming in de EU dat aan het Nederlandse wetgevingstraject voorafging, heeft zich zo goed als volledig buiten het blikveld van de Nederlandse democratische controle afgespeeld (Böhre 2010; Broeders 2011). Dit ondanks het feit dat hier de belangrijkste standaarden werden bepaald die de padafhankelijkheid van de paspoortwet zou bepalen. Over de vraag wie exact zich het gebrek aan parlementaire scherpte en kennis zou moeten aantrekken verschillen de opvattingen. Sommige nationale parlementariërs toonden zich in het verleden nogal teleurgesteld over het gebrek aan kritische houding van de Europese collega's: toenmalig PvdA- senator Jurgens verzuchtte dat het probleem met de Europese Unie is dat het Europees Parlement te weinig mensen bevat met een ingebouwde houding om waakzaam te zijn inzake mensenrechten en daardoor zelden sterke posities inneemt. Daar waar het Parlement wel actief is geworden, zoals bij de dataretentie komt dat "vrees ik, meer door de economische belangen van de providers die in de knel kwamen en minder vanwege de privacy-problematiek" (Jurgens 2005: 98). Maar ook in Den Haag liet men zich de Europese ambities soms ogenschijnlijk makkelijk aanleunen: "Compared to the critical attitude of the Dutch parliament with regard to the establishment of SIS I, the development of SIS II was discussed only marginally. On the few occasions when the Senate or the Second Chamber of parliament made an inquiry about SIS II, they rarely raised fundamental questions" (Brouwer 2008: 452). Bij tijd en wijle toonde het nationale parlement zich zeer kritisch, zoals bij de bewaartermijn voor verkeersgegevens. Op andere momenten legde het echter een grote volgzaamheid in de Europese arena aan de dag, zoals bij de inperking van de rechtsbescherming bij grensoverschrijdende gegevensuitwisseling ten behoeve van BTW-controle (Schenk-Geers 2007: 477).

Toch zijn er ook eerste indicaties dat er wellicht in Brussel een moment van bezinning komt in de tot op heden nauwelijks geremde ontwikkeling van meer en vooral vernetwerkte Europese datasystemen. Het Verdrag van Lissabon 'normaliseert' het beleidsterrein: de Europese instituties gaan hier nu ook op de traditionele manier functioneren, hetgeen een versterking betekent van de positie van het Europees Parlement en het Hof van Justitie. Het Europees Parlement liet inmiddels zijn tanden al zien in het Lissabon-tijdperk bij de behandeling en verwerping, begin 2010, van de afspraken tussen de EU en de Verenigde Staten inzake SWIFT.[10] In gesprekken met de Europese Toezichthouder voor Gegevensbescherming Hustinx[11] en met de Europeesrecht-deskundige Mitsilegas (Queen Mary University of London)[12], werd ook naar voren gebracht dat het nieuwe institutionele raamwerk wellicht een bepalende en conditionerende invloed op de inhoud gaat hebben. De relatieve beslotenheid waarin de Europese ministers van Justitie en Binnenlandse Zaken tot besluiten kwamen, wordt nu opengebroken. Welke vorm dat precies aan gaat nemen is nu uiteraard nog niet te zeggen.

5.1.5 LEIDENDE EUROPESE BELANGEN

Waar in de jaren tachtig en negentig van de vorige eeuw het belang van digitale (commerciële) dienstverlening bovenaan de Europese agenda prijkte en de EU-initiatieven om EDI (Electronic Data Interchange) te faciliteren elkaar in hoog tempo opvolgden (Mitrakas 1997), behoeft het geen nader betoog dat het belang van veiligheid en zeker ook de daarbij gevoelde urgentie, het afgelopen decennium de belangrijkste impuls is geweest voor de uitbouw van zowel de Europese systemen voor informatie-uitwisseling als de harmonisatie van maatregelen in de lidstaten. Of de veelheid aan maatregelen daadwerkelijk meer veiligheid heeft gebracht blijft ook op Europees niveau een weinig gestelde en onbeantwoorde vraag. Niet alleen omdat de hoeveelheid verijdelde aanslagen moeilijk te tellen is, maar ook omdat het materiaal voor een gedegen evaluatie veelal ontbreekt. Zo blijken de rapporten van Europol bijvoorbeeld volstrekt onvoldoende om de meer specifieke vraag te beantwoorden op welke punten politiële samenwerking en daarmee grensoverschrijdende uitwisseling van politiegegevens nu wel of niet voldoet en of zij in de toekomst al dan niet verder moet worden uitgebouwd (Fijnaut 2007: 137).

Maar niet alleen veiligheid stuwt de Europese digitale agenda in rap tempo voort. Het belangenpaar effectiviteit en efficiëntie speelt hier ook een prominente rol. Zo concludeerde de Europese Commissie in januari 2000 dat vormen van transparantie en rechtsbescherming bij fiscale inlichtingenuitwisseling, zoals die in sommige lidstaten zijn ontwikkeld, niet verenigbaar zijn met de toenemende behoefte aan efficiëntie bij het verkrijgen van internationale informatie (Schenk-Geers 2007: 5). Effectiviteit en efficiëntie (vertaald als kostenreductie en verbeterde toegang) zijn eveneens de leidende motieven bij de groeiende Europese aandacht voor interoperabiliteit. Eenvoudig gesteld staat interoperabiliteit voor de capaciteit van systemen om ‘met elkaar te praten’: te communiceren en gegevens uit te wisselen zonder verlies van betekenis van die gegevens. Het European Interoperability Framework uit 2004 voorziet in aanbevelingen voor zowel technisch beleid als de inhoud van de informatie en de interactie tussen overheidsinformatiesystemen van de lidstaten. In eerste instantie lag de prioriteit bij het realiseren (onder meer via pilots) van een pan-Europese standaardisatie van eOverheid applicaties op het terrein van dienstverlening en zorg, variërend van elektronische tolheffingssystemen, e-aanbesteding, elektronische handtekeningen en digitale patiëntendossiers (Ducastel 2008: 289). Maar inmiddels spreekt Europa de lidstaten ook aan op de winst die behaald kan worden met interoperabiliteit van politiesystemen (Verbeek 2010: 34), en wordt ook intersectorale interoperabiliteit gepromoot.[13] En daarmee is interoperabiliteit meer dan alleen van belang vanuit een oogpunt van effectiviteit en efficiëntie. Discussies in het Europees Parlement over interoperabiliteit tussen nationale politiële databanken laten zien dat het beleidsthema ook weer een directe link heeft met veiligheidsambities en daarmee politiek gevoelig ligt

(De Hert 2006). Ook de nadruk op interoperabiliteit en de noodzaak van data-uitwisseling in belangrijke verdragen op het gebied van Justitie en Binnenlandse Zaken, zoals het Verdrag van Prüm en het Den Haag Programma, wijzen op het grote politieke belang dat wordt gehecht aan informatiestromen voor veiligheid en opsporing (Broeders 2011).

Toch lijken in Europa de verankerende beginselen, in het bijzonder privacy, uit de schaduw te treden. In januari 2010 wees Eurocommissaris voor Justitie en burgerrechten, Reding, op het belang van gegevensbescherming. Ze benadrukte de noodzaak van één overkoepelend juridisch raamwerk voor een hoog niveau van gegevensbescherming in de EU. Dat raamwerk zou moeten gelden voor zowel de private als de publieke sector, met inbegrip van justitie en politie. In dit raamwerk moeten transparantie en eigen zeggenschap voor burgers een prominente plaats krijgen. Daarnaast zou de rol van de privacytoezichthouders versterkt moeten worden (Reding 2010). Zes maanden later voegde de Commissie een eerste daad bij het woord met de publicatie van de hiervoor genoemde Mededeling over het informatiebeheer van de Unie. Behalve een overzicht van alle bestaande maatregelen, presenteert de Commissie een raamwerk van inhoudelijke en procesmatige uitgangspunten voor de omgang met persoonsgegevens op het terrein van rechtshandhaving en migratie. Daaronder bevinden zich behalve bekende waarden en uitgangspunten als privacy, noodzakelijkheid en subsidiariteit ook: ‘gericht risicobeheer’ (risicobeoordeling moet zijn gebaseerd op bewijzen en niet op hypotheses), bottom-up beleidsontwikkeling (bij de ontwikkeling van nieuwe initiatieven moeten alle betrokkenen, zoals de nationale autoriteiten die het initiatief moeten uitvoeren, economische actoren en het maatschappelijk middenveld, vanaf een zo vroeg mogelijk stadium een inbreng hebben), evaluatie- en vervalbepalingen, en een duidelijke verdeling van verantwoordelijkheden. Opvallend bij de laatstgenoemde is overigens wel dat de Commissie met geen woord rept over heldere verdeling van verantwoordelijkheid wanneer burgers verstrikt raken in de digitale Europese wereld, maar het uitgangspunt uitsluitend duidt vanuit het belang van budgetoverschrijdingen en vertragingen ten gevolge van bijgestelde ambities en voorwaarden.“De ervaring met het SIS II-project leert dat het ontbreken van een duidelijke en stabiele beschrijving van overkoepelende doelstellingen, taken en verantwoordelijkheden in het beginstadium, kan leiden tot aanzienlijke kostenoverschrijdingen en vertragingen bij de invoering” (Europese Commissie 2010a: 30). Of verankerende en procesmatige beginselen de komende jaren ook inderdaad een volwaardige rol krijgen toebedeeld bij het vormgeven van de digitale Europese agenda valt moeilijk te voorspellen. In ieder geval staat voor 2011 de discussie en (naar verwachting) besluitvorming over een nieuw algemeen kader voor gegevensbescherming geagendeerd. Ter voorbereiding daarvan presenteerde de Europese Commissie op 4 november 2010 ‘een strategie voor versterking van de Europese gegevensbeschermingsregels’ met daarin voorstellen voor een modernisering van deze regels. De Commissie liet onder meer weten: “Iedereen heeft het recht te

worden 'vergeten', wanneer gegevens niet langer nodig zijn of wanneer iemand zijn gegevens wil laten wissen" (Europese Commissie 2010c: 1).

5.2 CONCLUSIE

Connectiviteit beperkt zich niet tot landsgrenzen. De opmars van ICT behelst schaalvoordelen die ervoor zorgen dat zich op Europees niveau beleidsmogelijkheden openen die letterlijk buiten het bereik van individuele lidstaten liggen. Door samenwerking op het niveau van informatie kunnen de lidstaten van de EU thema's oppakken die anders onhanteerbaar waren geweest. Een gemeenschappelijk migratiebeleid dat ook werkelijk operationeel gemeenschappelijk is (niet slechts op harmonisatie van wetgeving berust) is immers onbetaalbaar zonder de Europese migratiedatabanken. Recentelijk vindt er een verbreding van de blik plaats ten opzichte van de oorspronkelijke focus op asielzoekers en illegale vreemdelingen naar alle reizigers. Het feit dat ook informatie-uitwisseling ten behoeve van de interne markt in beeld is gekomen mag illustratief heten voor de volwassenwording van de informatiesamenleving. Maar duidelijk is ook dat er geen heldere afbakening is te geven van de aspecten van de eOverheid die de EU ter hand zou moeten nemen en de aspecten die bij de lidstaten belegd blijven.[14] De Europese overheid wijdt zich in ieder geval enthousiast aan de eOverheid en zal dat naar verwachting steeds meer doen.

Ook op bovenstatelijk niveau is een gezonde balans tussen stuwende, verankerende en procesmatige beginselen van belang. De migratiedatabanken zijn echte Europese applicaties, ten aanzien waarvan op statelijk niveau niets meer uit te balanceren valt. Op andere terreinen, zoals de uit Europa afkomstige privacywetgeving of de Verordening[15] die biometrie op het paspoort heeft geïntroduceerd, is sprake van een meer gelaagde structuur waarbij de nationale implementatie de balans nog wel degelijk kan veranderen. Ook uit de Europese initiatieven spreekt vooral een houding van vertrouwen in de technologie en vertrouwen in de opbrengsten die informatie-uitwisseling kan brengen. Het vaak onuitgesproken uitgangspunt is dat hoe meer uitwisselingen er worden mogelijk gemaakt, hoe beter de gecombineerde Europese overheden de vele uitdagingen waar zij voor staan het hoofd kunnen bieden. Eén uitdaging steekt met kop en schouders boven andere uit: het borgen van de veiligheid van Europese samenlevingen tegen de dreiging van het terrorisme. Het Europees Parlement vertolkt in deze houding vrij consequent een afwijkend geluid en is bijvoorbeeld bij discussies over gegevensuitwisselingen met de Verenigde Staten meermalen op de rem gaan staan. Tot voor kort had het Parlement echter veelal niet de mogelijkheid dan wel bevoegdheid om de discussie, laat staan het voorliggende voorstel, te wijzigen. Het bestaande Europese arsenaal van applicaties staat dan ook voortdurend onder druk om uitgebreid te worden, met informatiecategorieën en met participerende nationale en Europese organisaties.

ICT mag ook op Europees niveau dan inderdaad ongekende beleidsmogelijkheden hebben geopend, de oogst van dit beleid blijkt bijzonder moeilijk na te gaan. De evaluatiearmoede die in de Nederlandse context gesignaleerd werd, doet zich eveneens in Europa voor. Daardoor worden efficiëntie, effectiviteit en veiligheid enigszins ongrijpbare begrippen. Ook in Europa wordt het succes van een initiatief afgemeten aan de termen van het systeem zelf, bijvoorbeeld hoeveel ongewenste vreemdelingen in het SIS-systeem zijn genoteerd. De andere kant van het verhaal is dat de positie van burgers die zich in de Europese databanken opgenomen weten – en dat is een steeds grotere en 'normalere' groep burgers – uiterst zwak is. De wereld van deze databanken blijft voor hen verborgen, totdat men er tegenaan loopt bij een negatieve beslissing van een nationale autoriteit die gebaseerd is op een stukje digitale 'Europese' informatie, en dan is het bijzonder moeilijk de beslissing ongedaan te maken (zie onder meer Nationale Ombudsman 2010c). De verantwoordelijkheden voor herstel van foutieve of onrechtmatige informatie zijn bij deze databanken 'historisch' georganiseerd: een correctie moet bewerkstelligd worden bij de organisatie die de informatie oorspronkelijk noteerde, en dat kan in een andere lidstaat zijn geweest. Dit resulteert in een ondoordringbaar 'stelsel' van rechtsbescherming. De verankerende en procesmatige kanten van de *database state* zijn met andere woorden op het Europese niveau (nog) problematischer dan in Nederland. Dit is zorgwekkend vanuit het besef dat de Europese applicaties een steeds breder – en vanuit de positie van de gemiddelde burger gedacht alledaagser – bereik krijgen.

Ten slotte, 'de' Europese overheid wil naast gebruiker van ICT ook nadrukkelijk aanjager zijn, niet alleen van de industrie maar ook van het maatschappelijke gebruik van ICT. De inbreng van commerciële *stakeholders* is daarbij van groot belang, soms zelfs zodanig dat deze aan de tekentafel van een applicatie plaats mogen nemen. Zo zijn de *privacysettings* van het initiatief eCall door zuivere coöperatie tot stand gekomen. Hoe voordelig dit ook moge zijn voor de slagingskansen van een initiatief, zo ontstaat toch de paradoxale situatie dat de overheid soms ook voor haar 'core business', regulering, nog slechts aanjager is.

NOTEN

1 De afspraken werden neergelegd in het Prevention and Combating of Serious Crime (PCSC)-verdrag, dat eind 2010 nog ter goedkeuring aan het parlement moest worden voorgelegd. *Nederlands Juristenblad*, 2010, blz. 2731-2732.

2 Gesprek met mevr. S. in 't Veld, lid Europees Parlement, januari 2009.

3 NRC *Handelsblad*, 17 december 2010.

4 Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt, *Pb* L 376, blz. 36-68.

5 Beschikking 2008/49/EG van de Commissie van 12 december 2007 inzake de bescherming van persoonsgegevens bij de invoering van het informatiesysteem interne markt (IMI), *Pb* L 13, blz. 18-23.

6 Interview met de heer C. van Oranje, kabinet van EU-Commissaris Kroes, Brussel, maart 2010.

7 NRC *Handelsblad*, 20 december 2010.

8 Richtlijn 2006/24/EG, *Pb* L 105, blz. 54-63.

9 *Tractatenblad* 2001: 187.

10 De SWIFT-overeenkomst voorzag erin dat de VS toegang kregen tot (Europese) bankgegevens in het kader van de terrorismebestrijding. Het Europees Parlement verwierp deze overeenkomst wegens grote bezorgdheid over privacy, proportionaliteit en wederkerigheid.

11 Gesprek met EDPS, dhr. P. Hustinx, Brussel, maart 2010.

12 Gesprek met dhr. V. Mitsilegas, hoogleraar Europees strafrecht aan de Queen Mary University of London, mei 2010.

13 Besluit 2004/387/EG van het Europees Parlement en de Raad betreffende de interoperabele levering van pan-Europese *e*-overheidsdiensten, *Pb* L 181 [2004], blz. 25-35. Dit besluit spreekt van "horizontale" interoperabiliteit.

14 Dat wil zeggen: er is geen strijd te verwachten over de vraag of de EU wel bevoegd is om zich met aspecten van de eOverheid bezig te houden. Wel is steeds de vraag aan de orde of het Europese niveau het meest geëigende is voor een bepaald initiatief. De Nederlandse regering benadrukt dat dit lang niet altijd het geval is (Tweede Kamer 2010-2011c).

15 Verordening 2252/2004/EG van de Raad betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten, *Pb* L 385, blz. 1-6.

6 MARKTMEESTERS EN DE MARKT MEESTER ZIJN

Zonder het aanbod van de ICT-markt was er geen eOverheid. Demissionair minister Klink zond op 9 september 2010 een rapportage aan de Tweede Kamer die een indicatie geeft van de uitgaven aan de ICT-markt die met de eOverheid – in dit geval het EPD – zijn gemoeid.

"In juli is een Wob verzoek ontvangen van RTL Nederland waarbij gevraagd is om een compleet beeld te geven van 'alle kosten en activiteiten inzake het EPD bij of onder het Ministerie van VWS, anders dan reguliere departementaal ambtelijke kosten en activiteiten, waarvoor rekeningen zijn verstuurd dan wel waarvoor betaald is'. In de periode 2002 tot 1 juli 2010 is in totaal € 217,5 miljoen uitgegeven aan activiteiten met betrekking tot de invoering van de landelijke infrastructuur voor gegevensuitwisseling in de zorg (waaronder audits, adviezen, pilotprojecten, communicatie, IT, ontwikkeling en beheer, projectmanagement en instellings- en projectsubsidies Nictiz)" (Tweede Kamer 2009-2010g: 10).

Omgekeerd geldt ook dat de ICT-markt niet z'n huidige omvang zou hebben als de eOverheid niet zo'n vlucht had genomen. Voor de realisatie van alle ambities en plannen leunt en steunt de overheid sterk op een veelsoortig palet aan partijen van buiten de publieke sector. Wie kijkt naar de relatie tussen de overheid en de ICT-markt stelt vast dat deze langs drie lijnen is te duiden. Economisch, omdat de ICT-industrie een belangrijke sector is, en de overheid een partij van betekenis is voor spelers in die bedrijfstak (bouwers van systemen, ontwikkelaars van informatieapplicaties, consultants). Bestuurlijk, omdat de ICT-industrie fungeert als verlengstuk van het openbaar bestuur: de overheid giet de uitvoering van beleid in ICT-applicaties, en is daarvoor deels afhankelijk van aanbieders. Ten slotte regulatoir, omdat de overheid door regulering bij partijen op de ICT-markt een bepaald commercieel gedrag afdwingt. Zo kan de overheid besluiten spelregels aan de markt op te leggen wanneer een beperkt aantal spelers een zodanige informationele machtspositie heeft opgebouwd dat daardoor publieke belangen in het geding komen.

6.1 DE eOVERHEID ALS ECONOMISCHE KRACHT

6.1.1 DE INKOOP VAN DE eOVERHEID

ICT is een vitale en omvangrijke sector van de economie, zowel nationaal als internationaal. In 2007 draaide de top 250 van internationale ICT-bedrijven een omzet van 3,8 biljoen Amerikaanse dollars. De sector als geheel is bovendien een aanjager van innovatie. De investeringen in Research & Development (R&D) zijn hier vele malen hoger dan in sectoren als de autoindustrie of de farmacie, die traditio-

neel worden gezien als sectoren die sterk afhankelijk zijn van nieuwe ontdekkingen en innovaties. De ICT-sector investeert (wereldwijd) 130 miljard Amerikaanse dollars in R&D, waarvan 25 procent voor rekening komt van bedrijven uit de EU (alle cijfers OECD 2008). Met andere woorden: de ICT-industrie zorgt voor veel dynamiek, innovatie, economische groei en (hoogwaardige) banen. Dat betekent dat het voor de overheid een vitale en hoogwaardige industrie en kennissector is die 'gekoesterd' moet worden. ICT zorgt daarbij bovendien voor de noodzakelijke dynamiek en vernieuwing in maatschappelijke domeinen, wat voor het kabinet in 2008 aanleiding vormde om 54 miljoen euro beschikbaar te stellen als specifieke investeringsimpuls voor 'sectorale ICT-projecten in maatschappelijke domeinen'.[1]

Overheden zijn ook grote afnemers van ICT-producten. De vele eOverheid-projecten die door lokale, nationale, Europese en internationale overheden op de kaart worden gezet, moeten uiteindelijk – al dan niet via aanbestedingen – voor een belangrijk deel door ICT-bedrijven worden ontwikkeld en uitgevoerd. In 2007 rapporteerde het ministerie van BZK dat het rijk (inclusief baten-lastendiensten en ZBO's) in de periode 2000-2013 een ICT-gerelateerde projectenportfolio had die tot 5,8 miljard euro optelde, waarvan 4,1 miljard direct aan ICT werd besteed (Algemene Rekenkamer 2008a). De Algemene Rekenkamer (2008a: 29-30) kon op basis van deze gegevens echter geen inschatting per jaar maken en vermoedde bovendien dat de uitgaven eigenlijk hoger zijn. In het Verenigd Koninkrijk was de schatting vijf jaar geleden dat er per jaar 14 miljard pond aan *public sector IT* wordt uitgegeven (Dunleavy et al. 2006). Gezien de grote markt voor ICT bij overheden kan er, naast vraaggestuurde ontwikkeling, ook gesproken worden van een technologiepush. ICT-bedrijven zijn spelers van betekenis die, al dan niet met een ICT-consultant in de arm, actief de markt bewerken. Ook de overheid is er niet van gevrijwaard dat soms problemen worden gezocht en gedefinieerd vanuit een nieuw beschikbaar gekomen techniek of applicatievorm. Vertegenwoordigers van het CIO Platform Nederland gaven in gesprekken met de WRR aan dat de overheid – net als het bedrijfsleven – in de tang van een zeer beperkt aantal grote ICT-aanbieders zit, maar nauwelijks visie heeft hoe hiermee om te gaan.[2] Er is daarom alle aanleiding het opdrachtgeverschap te versterken via samenwerking tussen de overheid en het al evenzeer van ICT-leveranciers afhankelijke bedrijfsleven, aldus het CIO Platform Nederland.

Een gedeelte van de ICT-markt bij de overheid gaat schuil achter de voordeuren van de ministeries en uitvoeringsinstellingen en heeft alleen betrekking op de overheid zelf: salarissystemen, archiefsystemen, beveiliging en toegangspassen. Een ander deel van de ICT bij de overheid raakt direct, of indirect, aan de interactie met de burger. De afgelopen jaren zijn vele tientallen, zo niet honderden applicaties ontwikkeld op de beleidsterreinen van dienstverlening, zorg en controle. De meerderheid van die applicaties is (deels) ontwikkeld en gebouwd in nauwe

samenwerking met de private sector (Ministerie van EZ 2008). Soms blijken de specificaties van de aanbesteding zelfs zodanig ruim geformuleerd dat de externe partij aan wie de opdracht tot het ontwikkelen van een applicatie uiteindelijk wordt gegund, blijkt te kunnen bepalen welke actoren binnen de overheid bij de verdere ontwikkeling mogen aanschuiven.[3] Bij sommige initiatieven is de betrokkenheid van de markt op meer gebaseerd dan uitsluitend de concrete opdracht tot ontwikkeling, maar hebben de private spelers ook zelf een ambitie. Een voorbeeld hier is eCall: het initiatief om auto's in Europa te voorzien van elektronica die een handmatige of geautomatiseerde noodoproep uitzendt in geval van een ongeluk. De Europese Commissie zet op de ontwikkeling van eCall in om het aantal verkeersdoden op de Europese wegen sterk terug te dringen. Voor de nationale wegbeheerders is het een mooi initiatief om als bijkomstig doel het verkeersmanagement verder te optimaliseren: het omleiden van het verkeer in het geval van een ongeluk, of het aansturen van weginspecteurs ter plaatse. De nationale overheden onderzoeken andere toepassingen dan verkeersveiligheid (zoals opsporing) en een scala aan private partijen, variërend van de autoindustrie, mobiele telecommunicatie-exploitanten, private nooddiensten tot verzekeraars, stimuleert de ontwikkeling van eCall om omzet te verhogen, nieuwe producten te ontwikkelen of bestaande diensten efficiënter aan te bieden (Potters & De Vreeze 2010).

De grootste 'groeimarkt' voor ICT en andere technologische toepassingen bevindt zich in het veiligheidsdomein. Sinds de aanslagen in New York in 2001 zit de markt van databanken, biometrie en andere interne veiligheidssystemen en toepassingen sterk in de lift. De Organisation for Economic Co-operation and Development (OECD) sprak in een studie uit 2004 al over de *emerging security economy* (Stevens 2004) en Hayes (2009) spreekt van de groeiende 'Homeland Security market'. Duidelijk is in ieder geval dat het hier om groeimarkten gaat en dat bedrijven actief de markt opgaan om hun producten aan de man te brengen. In de OECD-studie uit 2004 werd de *security economy* geschat op een waarde van 100 miljard dollar (Stevens 2004). Op een iets kleinere schaal verwacht de International Biometric Group dat de markt voor biometrie tussen 2009 en 2014 groeit van 3,42 naar 9,37 miljard dollar. Vanwege de crisis wordt bovendien verwacht dat het grootste deel van de markt de komende jaren wordt bepaald door contracten van overheden (Biometric Technology Today 2009: 11). Met name de markt voor biometrie kent een aantal opvallende kenmerken. Gezien de grote verwachte groei is dit een internationale en zeer competitieve markt, maar ook een nog relatief jonge markt waarin standaarden en producten vaak nog niet goed uitgekristalliseerd zijn. Snijder (2010) laat zien dat de internationale biometrie-industrie sterk nationaal verkaveld is, waardoor innovatie grotendeels in handen is van de grote biometriebedrijven (dat zijn er wereldwijd rond de zes).

> "Deze grote bedrijven, die vanwege hun vertrouwelijke relatie met hun overheidsklanten en de beperkte uitwisselbaarheid van hun producten niet staan te wachten op nieuwkomers in de markt, hebben vanuit het handhaven van hun marktpositie geen voordeel bij verbeteren van de interoperabiliteit. En omdat innovatie veel geld kost en nieuwkomers op de biometrie markt niet snel grote overheidsprojecten krijgen toebedeeld, blijven strategische vernieuwingen op technisch vlak vaak liggen. De marktleiders innoveren wel, maar met name binnen de scope van hun eigen technologie" (Snijder 2010: 55-56).

Najaar 2010 ontstond de nodige onrust in de Tweede Kamer na berichten dat de minister van Justitie de bouw van de nationale databank voor biometrische kenmerken na een aanbestedingsprocedure had gegund aan 'een Frans commercieel bedrijf'.[4] Meerdere fracties uitten hun zorgen over het feit dat, aldus Heijnen (PvdA) "de centrale opslag als vanzelf ook in buitenlandse handen terecht kan komen" (Tweede Kamer 2010-2011a:3). Van Raak (SP):

> "Het lijkt mij toch heel erg logisch dat een Nederlands paspoort wordt gemaakt, beheerd, uitgegeven en gecontroleerd door de Nederlandse overheid. Er is echter weinig Nederlands meer aan het Nederlandse paspoort dat ik heb. De productie wordt uitbesteed. Het wordt gemaakt door een Frans commercieel bedrijf. De vingerafdruk die in het paspoort zit, wordt in een databestand opgenomen en ook dat wordt beheerd door een Frans commercieel bedrijf. Er zitten commerciële belangen bij en de AIVD heeft gewaarschuwd dat dit niet erg slim is, dat het uitbesteden van databestanden, van gevoelige informatie gevaarlijk kan zijn. Dat doet de AIVD toch niet voor niets?" (Tweede Kamer 2010-2011a: 3).

De staatssecretaris meldde naar aanleiding van de discussie dat wat betreft de ontwikkeling van de centrale administratie nog geen onomkeerbare stappen waren gezet (Tweede Kamer 2010-2011a).

Naast een technologiemarkt voor de ontwikkeling van applicaties is er een informatiemarkt waarop evenzeer grote winsten worden gemaakt. Het verzamelen en bewerken van informatie voor de verkoop of het gebruik van informatie voor *targeted advertising* is een zeer lucratieve onderneming. Google, de ongekroonde koning van het verzamelen, koppelen en verrijken van persoonsinformatie om adverteerders te bedienen, rapporteerde voor het eerste kwartaal van 2010 een omzet van 6,77 miljard Amerikaanse dollar.[5] Ook de informatiemarkt is voor de overheid waardevol. Niet alleen omdat bedrijven in opdracht van de overheid databases vullen, maar ook omdat de overheid al jarenlang gretig gebruikmaakt van de schat aan informatie die in de private sector wordt verzameld.

6.1.2 de ict-'markt' binnen de overheid

Maar niet alleen commerciële spelers bouwen aan de eOverheid. De overheid ontwikkelt ook in eigen huis. Zo is een kerntaak van het Nationaal ICT Instituut in de Zorg (Nictiz) "de ontwikkeling van en de keuze voor de specificaties voor de landelijke generieke zorg infrastructuur en het EPD (inclusief de te hanteren standaarden)" (Pluut 2010:14). De belangrijkste bouwer binnen de overheid is de stichting ICTU (ICT Uitvoeringsorganisatie) die in 2001 door het ministerie van BZK en de VNG werd opgericht om kleine en grote ICT-projecten voor overheden te ontwikkelen (Van Loon 2010). Wie naar deze en andere publieke bouwers kijkt, stelt overigens vast dat commerciële ICT-ontwikkelaars vaak binnen de muren van de overheid verder aan de eOverheid werken (Horrocks 2009). In de dagelijkse praktijk blijkt dat bij veel ICT-projecten en bij grote uitvoeringsinstanties zoals de Belastingdienst grote aantallen commerciële ontwikkelaars en externe consultants worden betrokken. Een artikel op webwereld.nl dat op basis van een Wet openbaarheid van bestuur (Wob)-verzoek bij het ministerie van BZK de aantallen en verhoudingen tussen ambtenaren en externe ICT'ers in kaart bracht, kreeg de suggestieve en veelzeggende titel 'Rijks-ICT blijkt walhalla voor huurlingen'.[6] Ook voor ICTU zelf geldt dat het personeelsbestand voor het overgrote deel bestaat uit extern ingehuurde krachten, hetgeen de organisatie zelf verklaart vanuit de wens om met de werkvoorraad mee te groeien en krimpen.[7] In de dagelijkse gang van zaken betekent dit vaak dat de ambtenaar die vanuit een vakdepartement verantwoordelijk is voor een ICT-project zaken moet doen met een uitstekend in de technologie ingevoerde externe projectmanager die een groot team tot zijn beschikking heeft. Er is kortom sprake van een grote kennisasymmetrie.

6.2 de ict-markt als bestuurlijk verlengstuk

6.2.1 problematisch opdrachtgeverschap

Bij veel eOverheidprojecten blijkt het scherp en professioneel aansturen van ontwikkelaars niet eenvoudig. Deels komt dit voort uit de (beperkt) beschikbare technologische kennis bij de overheid en ook is het terug te voeren op het niet altijd professionele opdrachtgeverschap en de opvattingen daaromtrent.[8] Zo staakte het ministerie van Justitie najaar 2010 zijn ICT-project Cajis, dat bij de Dienst Justitiële Inrichtingen (DJI) zou moeten gaan fungeren als gevangenis-informatiesysteem. Het project, waaraan in 2009 en 2010 al 12 miljoen euro is uitgegeven, werd gestopt omdat het te veel doelstellingen kreeg en dus onbestuurbaar was geworden.[9] Eerder leverden ICT-projecten als C2000, Toeslagen bij de Belastingdienst en Walvis grote problemen op. Over dit laatste project merkte voormalig Nationaal Ombudsman, nu staatsraad bij de Raad van State Oosting op: "In het geval van Walvis zijn we ofwel met zijn allen veel te optimistisch geweest, ofwel de wetgever heeft remmende adviezen grandioos in de wind geslagen" (Februari 2008: 91).

Meerdere rapporten van de Algemene Rekenkamer laten zien dat er wat betreft kosten, planning en de doelmatigheid van ontwikkelingstrajecten veel te verbeteren valt.[10] De Rekenkamer constateert dat projecten vaak te ambitieus en te complex blijken te zijn, waardoor de kosten en doorlooptijden nogal eens uit de hand lopen en de opgeleverde resultaten niet altijd aan de verwachtingen voldoen (Algemene Rekenkamer 2007a). Deze constatering geldt zowel voor grote Nederlandse projecten (Algemene Rekenkamer 2007a, 2008a; Snijders 2011; Pluut 2010) als voor Europese projecten als het Schengen Informatiesysteem II of het VIS (Broeders 2011). De Socialistische Partij bracht in 2008 aan de hand van 350 meldingen over 'ICT-verspilling' een grote diversiteit aan problemen in beeld, variërend van aanbestedingsperikelen, belangenverstrengeling tussen overheid en markt, slechte communicatie, grootheidswaan in de politiek en gebrek aan kennis (SP 2008). Voorjaar 2010 meldde het Adviescollege toetsing administratieve lasten (Actal) in een brief aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties dat vanwege het ontbreken van sturing op de inzet van ICT, 500 miljoen euro aan besparing op de administratieve lasten niet wordt gerealiseerd (Actal 2010).

Een relevante factor bij de problematiek betreft de zichtbare spanning tussen de wensen die uitvoerende instanties hebben over ICT en de daadwerkelijk ontwikkelde systemen die het resultaat zijn van de tekentafel van de beleidsdepartementen. Het komt zelden voor dat de uitvoerende diensten, de eindgebruikers, vroeg in het proces van ontwikkeling betrokken worden. Vaak worden ze in het geheel niet betrokken en wordt het systeem kant en klaar afgeleverd of, oneerbiediger gezegd, over de schutting geworpen (Van Loon 2010). Breed gedragen – van politie, Belastingdienst, partners in de Manifestgroep tot Logius – is de opvatting dat uitvoerders veel te weinig en veel te laat worden betrokken bij de ontwikkeling van systemen en applicaties. De kloof tussen het niveau van de overheid als opdrachtgever (veelal een ministerie) en de overheid als feitelijk gebruiker van een ontwikkeld systeem (uitvoeringsniveau) is daarmee vaak groot.[11] Deze discrepantie tussen beleidsambities en praktische implementatie valt ook te illustreren met de invoering van het biometrisch paspoort. De introductie van het beleid loopt jaren vooruit op de controle-infrastructuur die nodig is om die biometrische paspoorten aan de grens daadwerkelijk te gebruiken (Böhre 2010).

Op een schaalniveau hoger, dat van de digitale grenzen van de Europese Unie, is de discrepantie tussen het beleidsniveau van hoogstaande digitale en biometrische databanken en de dagelijkse gang van zaken aan de buitengrenzen van de EU nog veel groter.[12] Wanneer een systeem 'af' is, wordt op verschillende niveaus in de politiek en binnen de overheid heel anders gedefinieerd. Zeker als de lijnen tussen politiek en de uiteindelijke uitvoering erg lang zijn, is de neiging om succes (en falen) te definiëren op het systeemniveau: als het systeem operationeel is, wordt het project als een succes gezien. Vaak is dat ook in de aard van de evaluaties terug

te zien. De schaarse evaluaties van het Eurodac-systeem, dat meervoudige asielaanvragen in de EU moet detecteren, laat de informatiestromen en de 'hits' tussen de lidstaten keurig zien, maar zwijgt over of en wat er met die informatie wordt gedaan in de zin van het overdragen van asielmigranten tussen de lidstaten. De systeemlogica domineert in aandacht en bepaalt de 'uitkomst' van de evaluatie (Broeders 2011).

Het opdrachtgeverschap wordt ook bemoeilijkt doordat 'de' overheid zeker niet bestaat als het om de wensen en verwachtingen voor ICT gaat, wat alleen al blijkt uit de constatering van de Algemene Rekenkamer dat juist de politieke dynamiek tussen minister, Tweede Kamer en departement vaak een belangrijke reden is voor het mislukken of vertragen van grote ICT-projecten. De dynamiek tussen de Raad van Ministers, de Commissie en, zeker na de inwerkingtreding van het Verdrag van Lissabon, het Europees Parlement genereert in Europa een vergelijkbaar beeld van voortdurend veranderende politieke eisen aan een systeem in ontwikkeling, gecombineerd met onrealistische deadlines (Broeders 2011).[13] Relevant is ook de grote afstand tussen de departementen, die vaak als opdrachtgever functioneren, en de bouwers van systemen. De al eerdergenoemde Gateway Review NUP plaatste grote vraagtekens bij de kwaliteit van het opdrachtgeverschap vanuit de vakdepartementen: "wanneer het gaat om dergelijke enorme projecten, is er gerede twijfel of de bemensing van de overheid in het algemeen en die van de opdrachtgevende departementen in het bijzonder, goed is toegerust voor zaken als project- en programmamanagement" (Gateway NUP 2009: 2). Gesprekspartners van de WRR menen bovendien dat er te veel vanuit het belang van projectmanagement op concrete initiatieven wordt gewerkt en te weinig aandacht is voor projectoverstijgende aspecten die de eenheid van beleid en uitvoering raken.[14] Aspecten als juridische randvoorwaarden en rechtsbescherming van burgers zijn zaken die bestuurders aangaan en niet projectmanagers, aldus Wijntje en Peereboom (Financiën/Belastingdienst). Door de focus op individuele projecten en sturing vanuit de beperkte optiek van bedrijfsvoering ontbreekt het ook aan lerend vermogen en een visie op de samenhang tussen initiatieven, aldus beide gesprekspartners.

Illustratief voor de problemen is de situatie rondom de eerdergenoemde stichting ICTU. Vanuit een departement wordt vaak met onvoldoende inzicht in de materie en onvoldoende scherpte een opdracht geformuleerd.[15] In het licht van het welslagen van grote ICT-projecten is het ook problematisch dat ICTU, in zijn eigen woorden, een echte projectorganisatie is. Als een project af is, verdwijnt het bij ICTU van de agenda (Van Loon 2010). Vaak moet dan de echte afstemming met de dagelijkse praktijk nog beginnen. Bovendien zijn systemen nooit af, maar zullen ze beheerd en doorontwikkeld moeten worden. Voor het beheer van diverse eOverheidsystemen is in 2006 GBO.Overheid opgericht, dat later tot Logius is omgedoopt.[16] In de praktijk neemt deze organisatie het systeem over van ICTU en

verzorgt vervolgens, namens de overheid, het beheer. Een beleidsdepartement is daarmee opdrachtgever van zowel ICTU als Logius, waarbij Logius in feite de afnemer van het systeem is. De onderlinge afstemming tussen deze organisaties is echter (nog) heel beperkt. Pas relatief recent probeert men vanuit het ministerie van BZK tot een meer structurele samenwerking en afstemming tussen de partijen te komen.[17] In deze complexe context van opdrachtgeverschap, ontwikkeling, beheer en doorontwikkeling is het lastig om na te gaan wie er precies verantwoordelijk is voor de vertaling van de beleidsambitie in het daadwerkelijke systeem: veel keuzes worden immers in de programmatuur gemaakt en lopende de tijd ook voortdurend gemaakt. De controle op verantwoordelijkheid is in de feitelijke praktijk niet of onvoldoende duidelijk belegd.

6.2.2 CHIEF INFORMATION OFFICER (CIO) ALS PROBLEEMOPLOSSER

Een overheid die innoveert en daarmee ook de nieuwe mogelijkheden van digitalisering benut voor de uitvoering van beleid, beweegt zich onherroepelijk op een speelveld waarvan de contouren niet op voorhand zijn gegeven. Gezien deze dynamiek is het daarom onvermijdelijk dat het pad van digitalisering gepaard gaat met zowel geslaagde als mislukte projecten. Innovatie zonder risico bestaat immers niet. Belangrijk daarbij is wel dat er geleerd wordt en kan worden van zowel de successen als de mislukte projecten, maar aan die voorwaarde blijkt vaak nog onvoldoende voldaan. Om tot een betere sturing op projecten te komen adviseerde de Algemene Rekenkamer het kabinet enkele jaren geleden de functie van de Chief Information Officer (CIO) bij de rijksoverheid in te stellen. Deze persoon zou ook een rol moeten krijgen bij het tijdig en adequaat informeren van het parlement over de voortgang van ICT-projecten (Algemene Rekenkamer 2008a: 53). Ervaringen in de Verenigde Staten met de verplichte aanstelling van een CIO, die op het hoogste niveau in de ambtelijke organisatie wordt gesitueerd, laten namelijk een sterke vooruitgang in de voortgang van projecten zien (Petri 2008). Ook andere landen, waaronder Oostenrijk en het Verenigd Koninkrijk, hebben de functie van de CIO ingevoerd. Het kabinet gaf uitvoering aan de suggestie en inmiddels kent ons land zowel een centrale en coördinerende Rijks-CIO als CIO's bij departementen. Diverse uitvoeringsinstanties en een enkele gemeente hebben dat voorbeeld inmiddels gevolgd (Snijders 2011). De Rijks-CIO is verantwoordelijk voor de sturing van de werkzaamheden van de CIO's op rijksniveau. Het is de bedoeling dat een CIO onder meer de ambtelijke en politieke leiding gevraagd en ongevraagd adviseert over grote ICT-projecten. Van groot belang zijn dan een goede relatie en wisselwerking tussen de CIO en beleidsbepalers. Een knelpunt zit in ieder geval in de reikwijdte van het werkveld van de CIO. De meeste en grootste ICT-projecten spelen veelal bij ZBO's of andere uitvoeringsorganisaties die op afstand van het departement staan (Snijders 2011). Ook heeft hij geen invloed op regionaal en lokaal niveau, terwijl grote ICT-projecten, zoals bijvoorbeeld de Verwijsindex Risicojongeren, dwars door alle bestuurslagen heen lopen en inter-

fereren met activiteiten op rijksniveau. De CIO is in de praktijk vooral bezig de ICT-projecten beheersbaar te houden en komt niet of nauwelijks toe aan de rol van informatiestrateeg en trendwatcher. Hierdoor is het risico aanwezig dat de CIO eindigt met een aanzienlijke, maar onderschatte verantwoordelijkheid, in het beste geval enig gezag, maar geen macht. In ieder geval heeft het kabinet-Rutte in het regeerakkoord afgesproken het toezicht op grootschalige informatiseringsprojecten en het oplossen van automatiseringsproblemen structureel aan te gaan pakken (Regeerakkoord 2010: 42).

6.2.3 beleid als systeemontwerp

Dunleavy et al. (2006: 61) zien Nederland als een typische, en ver doorgevoerde, poldervariant van het Europese Rijnlandse model als het gaat om de samenwerking tussen overheden en ICT-bedrijven. Een 'goede verstandhouding' en 'consensus en wederzijdse ondersteuning' staan daarin centraal, hetgeen contrasteert met het Angelsaksische model waarin outsourcing en financiële controle voorop staan. In de context van een hechte samenwerking tussen overheid en ontwikkelaars en adviseurs is het lastig om na te gaan wie er precies richting geeft aan de wisselwerking tussen beleidsambities en de inrichting van het daadwerkelijke systeem. Daar waar de eOverheid gestalte krijgt in een sterke interactie tussen de overheid als opdrachtgever en marktpartijen als ontwikkelaars en ondersteuners, is de ICT-markt een verlengstuk van het bestuur: op meerdere momenten in het proces van totstandkoming van systemen worden in feite belangrijke bestuurlijke en beleidskeuzes gemaakt dan wel 'voorgeprogrammeerd'. Dit wordt nog versterkt door de recente populariteit van zogenaamde Privacy Enhancing Technologies (PETs), waarop in een volgend hoofdstuk (paragraaf 7.1) nader wordt ingegaan (vgl. Article 29 Data Protection Working Party & Working Party on Police and Justice 2009: 12). PETs werken volgens de logica dat de verankeringen van en grenzen aan de technologie in de applicaties zelf ingebouwd worden. Zodoende wordt de inzet voor het opdrachtgeverschap verhoogd, want de overheid zal garanties via PETs zelf duidelijk in de opdracht over moeten brengen. Dit terwijl de prioriteiten van de overheid er eerder vaak anders uitzien. Systeemontwerpers zoals CapGemini houden, door ervaring wijs geworden, in het ontwerp van de software rekening met de nog niet expliciet geformuleerde politieke wensen om informatiestromen te combineren of juist te scheiden. De 'schotten' die zij tussen informatiebronnen inbouwen, zijn zo gemaakt dat ze eenvoudig te verwijderen of te versterken zijn als daar later om wordt gevraagd. Op deze wijze wordt bevorderd dat bij voortschrijdend inzicht of een gewijzigde politieke koers onnodige kosten kunnen worden voorkomen.[18]

De interactie tussen systeemontwikkeling en beleidskeuzes is niet alleen op rijksniveau zichtbaar. Met de keuze om bepaalde ontwikkelingen voor een belangrijk deel ook op lokaal niveau neer te leggen, zoals de initiatieven binnen de jeugdzorg,

ontstaat feitelijk ruimte voor systeemontwikkelaars om de eOverheid te sturen (Keymolen & Prins 2011). Waar op centraal niveau een organisatie als ICTU, beschikkend over veel professionele kennis en ressorterend onder bestuurlijke verantwoordelijkheid en toezicht van het ministerie van BZK, een landelijk systeem opbouwt, moeten gemeenten of regio's voor hun lokale variant zelf in zee gaan met (semi)commerciële partijen, waarbij de publieke controle op de beleidsbeïnvloeding door deze partijen summier te noemen is. Maar uiteindelijk zijn het wel deze systemen die de categorieën maken die bepalend zijn voor de burgerbeelden die de overheid hanteert. Vertrekkend vanuit het adagium dat 'categorieën politiek zijn', is het van belang te weten waar en door wie deze gemaakt worden.

6.2.4 KWARTIERMAKERS

"De 'plek van de macht' wordt daarom – in letterlijke en figuurlijke zin opgevat – door informatisering eerder voller dan verlaten" (Van de Donk 1997: 502). Op die plek van de macht figureren steeds vaker ook 'kwartiermakers': organisaties, stichtingen en agentschappen die, al dan niet specifiek voor de gelegenheid ingesteld, veel van de vitale (beleids)beslissingen in het ontwikkeltraject nemen, zonder veel directe (democratische) controle daarop. Voorbeelden zijn de stichting EKD.NL (voor de ontwikkeling van het EKD – Keymolen en Prins 2011), Stichting Nictiz voor het EPD (Keizer 2011; Pluut 2010) en het Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) dat een vitale rol speelde bij de vormgeving en communicatie over de ontwikkeling van het Nederlandse biometrische paspoort (Böhre 2010; Snijder 2010). Ook de geschiedenis van de Europese Verordening voor het biometrisch paspoort laat zien dat de ontwikkeling van standaarden en andere belangrijke keuzes zijn genomen in onverwachte werkgroepen (in dit geval the Visa Working Party), *alle* bezwaren van het Europees Parlement werden genegeerd en het uiteindelijke voorstel is afgehamerd door de General Affairs and External Relations Council. Met andere woorden: niet de ministers van Justitie en Binnenlandse Zaken die het hele voortraject hebben gedaan, maar de ministers van Buitenlandse Zaken hebben het voorstel in een verordening omgezet (Broeders 2011; zie Aus 2008 voor een gedetailleerde weergave van het proces). Vaak ver buiten het blikveld van Nederlandse burgers en hun verkozen vertegenwoordigers werden besluiten over techniek, standaarden en informatie-uitwisseling genomen die doorwerken in de technologie die uiteindelijk wordt gebruikt en in de informatie die tussen overheden wordt uitgewisseld. De keuze voor en afspraken over gezichtsherkenning en vingerafdrukken op het paspoort die door de International Civil Aviation Organization (ICAO) zijn vastgelegd, waren het resultaat van ouderwets spierballenwerk van een beperkt aantal grote staten in de kaders van de G8, de informele Europese Group of Five, EU-werkgroepen en de ICAO (Aus 2008). De vormgeving van de applicatie eCall vond plaats in een ad-hocwerkgroep, de eCall Driving Group, die 144 deelnemende organisaties telde, waarvan het leeuwendeel commercieel was (eCall

Driving Group 2005). De verwachting is dat de Europese Commissie deze uitkomsten in wetgeving zal omzetten (Potters & De Vreeze 2010).

6.3 VERANTWOORDELIJKHEID VOOR DE ICT-MARKT

Een derde en laatste lijn waarlangs de interactie tussen de overheid en de ICT-markt valt te duiden is die van de verantwoordelijkheid die de overheid heeft voor wat er zich op deze markt afspeelt. Daarbij is de ICT-markt overigens veel ruimer dan uitsluitend de wereld van de bouwers en ontwikkelaars van systemen. Het gaat dan ook om de informatiegiganten die hun businessmodel op de persoonsgegevens van (Europese) burgers bouwen, maar ook om telecommunicatie- en internetaanbieders die netwerkverkeer niet langer gelijk behandelen en onderscheid maken (in tarieven, exclusiviteit of snelheid van doorgifte) tussen bepaalde diensten en toepassingen (het schenden van de zgn. netwerkneutraliteit). Dat overheden zich deze verantwoordelijkheid lijken aan te trekken blijkt onder meer uit de stap van de Federal Communications Commission (FCC) in de VS tot het afdwingen van netwerkneutraliteit[19] en de mededeling van Europees Commissaris Kroes dat het toezicht op Social Networking Sites en de daarin gehanteerde privacy settings verscherpt gaat worden, in het bijzonder waar het gaat om jeugdigen (Kroes 2010). Waar de Europese Commissie in het domein van de ICT eerder zijn pijlen richtte op het monopolie van een grote ontwikkelaar (Microsoft), komen nu de informatiegiganten als Google en Facebook in beeld. Burgers moeten in bescherming worden genomen tegen een agressieve en competitieve informatiemarkt, zo lijkt de teneur. Illustratief voor de discussie over de verantwoordelijkheid van de overheid is ook de opvatting van het ministerie van Justitie over de toepassing van biometrie in de private sector: “De aspecten waar de overheid rekening mee houdt ten aanzien van biometrie in de publieke sector kan zij ook van toepassing verklaren op de private sector in haar rol als beschermer van de belangen van de burger en de maatschappij” (Ministerie van Justitie 2010: 33). Juist op het terrein van identiteitsmanagement lijkt een rol voor de overheid aangewezen, zo merken diverse gesprekspartners van de WRR op. Deze observatie sluit aan bij de zorgen die burgers hebben over het gebruik van identificatie-instrumenten door de private sector. De resultaten van de in opdracht van ECP-EPN en de WRR uitgevoerde enquête laten zien dat burgers sterke bedenkingen hebben tegen een breed gebruik van het BSN en biometrie in het maatschappelijk verkeer (Attema & De Nood 2010: 2). Bij de argumenten wordt de kans op fraude genoemd. Verder blijken burgers grote moeite te hebben met het gebruik van het BSN door zorgverzekeraars. De meningen over het gebruik van dit nummer door banken blijken sterk verdeeld (Attema & De Nood 2010: 2). Ook ander onderzoek laat zien dat burgers zich zorgen maken over risico’s die digitalisering meebrengt, zoals financiële fraude op internet en diefstal van identiteiten (Van Deursen & Van Dijk 2010: 63).

Interventie door de overheid kan ook ingegeven worden door de prijs die de overheid zelf betaalt, bijvoorbeeld via de kosten van opsporing in gevallen van fraude met identiteiten.[20] Daarnaast heeft de overheid de positie en verantwoordelijkheid om (technologische) onveiligheid aan te pakken. De overheid kan identiteitssystemen en sleutels net zomin als marktpartijen voor de volle honderd procent beveiligen, maar heeft wél, en hierin verschilt ze van marktpartijen, de doorzettingsmacht om de afwenteling van onveiligheid te reguleren. De overheid kan, met andere woorden, voorschrijven welke schouders bepaalde risico's moeten dragen. Binnen deze arrangementen kunnen de kosten en baten van de onveiligheid worden afgewogen en verantwoordelijkheden aan de betrokken actoren worden toebedeeld (Van Eeten 2011). Burgers zijn dan niet langer uitsluitend op zichzelf aangewezen om eventuele problemen die voortkomen uit de onveiligheid van identiteitssystemen op te lossen.

Een nadrukkelijker bemoeienis met de ICT-markt kan ten slotte aan de orde zijn als de effecten van het gebruik van digitale technieken over de grenzen van de private sector heen in het publieke domein gaan spelen. Illustratief is hier digitale identiteitsbepaling. Momenteel is nauwelijks sprake van regulering of zelfs maar politieke aandacht voor het gebruik en de kwaliteit van digitale identiteiten in de private sector. Zwembaden, supermarkten, werkgevers en computerfabrikanten experimenteren bijvoorbeeld volop met nieuwe toepassingen van biometrische identiteitsbepaling. Hoe het met (garanties voor) de kwaliteit hiervan is gesteld blijft echter onduidelijk. Nu de praktijk laat zien dat bij het gebruik van identiteiten de grenzen tussen de publieke en private sector steeds diffuser worden (Van de Hof et al. 2009), zijn er serieuze risico's dat ook de kwaliteit van de identiteitsbepaling door de publieke sector verwatert, aldus diverse gesprekspartners.

6.4 CONCLUSIE

De overheid is de belangrijkste afnemer van ICT-producten, maar omgekeerd geldt ook: ICT is een van de belangrijkste instrumenten aan het worden bij de vormgeving van beleid. Aldus zijn degenen die de producten ontwikkelen onmisbare vormgevers en is het opdrachtgeverschap daarmee een scharnierpunt in de ontwikkeling van de eOverheid. De balans tussen de stuwende, verankerende en procesmatige beginselen zou mede binnen dit opdrachtgeverschap voor de eOverheid tot stand moeten worden gebracht. Het voorgaande laat zien dat het bij de ontwikkeling van applicaties en koppelingen echter bij de overheid vaak ontbreekt aan gedifferentieerde kennis en expertise, waardoor het moeilijk wordt om de verwachtingen ten aanzien van wat ICT vermag van meer kritische lading te voorzien. Ook lijkt er nauwelijks sprake van een besef dat opdrachtgeverschap vergezeld moet gaan van een realistische blik op de merites van de stuwende beginselen. De overheid mist mensen die een besef van bestuurlijke verantwoordelijkheden kunnen handhaven te midden van een bazaar aan technische mogelijkheden en

hun pleitbezorgers. Opdrachtgeverschap en de verankerende beginselen blijken onvoldoende met elkaar in verbinding te brengen, omdat bijvoorbeeld een helder idee ontbreekt over de wijze waarop technologisch ingebouwde normen (Privacy Enhancing Technologies) zich verhouden tot normen in het recht en de samenleving. De procesmatige kwaliteit van het opdrachtgeverschap ten slotte vertoont ook lacunes, in het bijzonder in de gebrekkige professionalisering en de beperkte mogelijkheden tot participatie en inbreng van eindgebruikers bij de ontwikkeling van applicaties.

Te midden van de 'bestuurlijke drukte' van instanties die aan de basis staan van de voortdurende ontwikkeling van de eOverheid is het opvallend dat het beleidsdiscours ten aanzien van de ICT-markt en maatschappelijk gebruik van ICT vrijwel geheel in het teken blijft staan van facilitering. De industrie moet worden gefaciliteerd omwille van haar grote economische macht, bijdrage aan het Bruto Binnenlands Product (BBP) en de werkgelegenheid, en wellicht zelfs vanwege haar vermogen om de activiteiten te verplaatsten naar een ver land. De overheid moet zichzelf zo goed mogelijk van technische faciliteiten voorzien die zij inkoopt op de ICT-markt. Ten slotte moet de burger worden gefaciliteerd om zijn productiviteit te verhogen. Hoe belangrijk die zaken ook zijn, vastgesteld kan worden dat er geen structurele aandacht uitgaat naar de verantwoordelijkheid van de overheid voor de ontwikkelingen op de ICT-markt en de maatschappelijke impact daarvan. Het ongereguleerd gebruik van biometrische identiteitsbepaling door particulieren is een illustratie van deze lacune in de beleidsaandacht.

NOTEN

1 http://regelingen.agentschapnl.nl/content/ict-impuls.
2 Interview met dhr. H. Wesseling (TNT Post), dhr. H. Grevelman (ZwitserLeven), dhr. P. Hagedoorn (3Align Information Governance), dhr. F. Krom (ING), dhr.T. Mekel (Athlon Car Lease), januari 2009.
3 Interview met dhr P. Wijntje en dhr. S. Peereboom, ministerie van Financiën en Belastingdienst, september 2010.
4 *de Volkskrant*, 15 september 2010. Dat een Frans bedrijf de Nederlandse paspoorten ontwikkelt, is overigens een logisch gevolg van de eerdere privatisering van de Sdu.
5 http://investor.google.com/earnings/2010/Q1_google_earnings.html.
6 http://webwereld.nl/nieuws/65143/rijks-ict-blijkt-walhalla-voor-huurlingen.html.
7 http://www.ictu.nl/index.php?option=com_content&task=view&id=684&Itemid=26.
8 Interviews met mevr. E. Bogerman, ICTU, januari 2009; dhr. A. Thijssen en mevr. T. Timmermans, ministerie van BZK, oktober 2009.
9 *Computable*, 6 september 2010.
10 Zie bijvoorbeeld Algemene Rekenkamer (2003) over het C2000-systeem, (2007b) over het P-Direct-systeem voor personeelsadministratie, (2008b) over het ICT-project huur- en zorgtoeslag en (2007b en 2008b) over de lessen uit grote ICT-projecten.
11 Gesprek met dhr. W. van Vemde, korpschef politie Gooi- en Vechtstreek, november 2009; gesprek met dhr. A. Thijssen en mevr. T. Timmermans, directie Dienstverlening, Regeldruk en Informatiebeleid, ministerie van BZK, oktober 2010; interview mevr. S. Borgers, CIO VROM, december 2009. Zie ook Actal 2010.
12 Aldus Monica Gariup, Research Officer bij Frontex, EU Border Management Agency tijdens de conferentie over het voorgenomen Europese Entry/Exit-systeem in Brussel (4 november 2009).
13 Dhr. F. Paul, verantwoordelijk voor de grote Europese migratiedatabanken binnen de Europese Commissie schetste eenzelfde beeld (gesprek januari 2009), evenals dhr. P. Hustinx, de European Data Protection Supervisor (gesprek maart 2010).
14 Interview dhr. P. Wijntje en dhr. S. Peereboom, ministerie van Financiën en Belastingdienst, september 2010.
15 Onder meer aangekaart in het interview met mevr. T. Timmermans en dhr. A. Thijssen, ministerie van BZK, oktober 2010, en mevr. S. Borgers, CIO van het ministerie van VROM, december 2009.
16 “De naam Logius is afgeleid van logisch. Hij zegt iets over de wijze waarop de producten en diensten van GBO. Overheid met elkaar in verband staan, en dat ze verbindingen mogelijk maken”, aldus de website.

17 Interview met dhr. A. Thijssen en mevr. T. Timmermans, directie Dienstverlening, Regeldruk en Informatiebeleid, ministerie van BZK, oktober 2010.
18 Gesprek met dhr. N. Kaptein, CapGemini, juni 2009.
19 http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db1221/DOC-303745A1.doc
20 Gesprek met dhr. J. Stam, ministerie van Justitie, mei 2010.

7 CONTROLEURS VAN DE eOVERHEID

In de voorgaande hoofdstukken zijn veel van de 'controleurs van de eOverheid' al de revue gepasseerd: instanties die tot taak hebben om aspecten van de informatisering van de relatie burger-overheid te toetsen, waar nodig bij te stellen en/of aan te dringen op bijstelling. In dit hoofdstuk wordt de taakstelling van deze instituties in relatie tot de digitaliseringsinitiatieven van de overheid nader onder de loep genomen. Maar de aandacht gaat vooral uit naar hun taakopvatting en de feitelijke invulling daarvan. Diverse actoren hebben en vervullen een rol als kritisch volger van de eOverheid en vormen daarmee een essentieel onderdeel van het noodzakelijke systeem van *checks and balances*. De Raad van State, het College Bescherming Persoonsgegevens (CBP), de Nationale Ombudsman, de Algemene Rekenkamer en – in beperkte mate – de rechterlijke macht: allemaal hebben ze zich de afgelopen jaren tot meer of minder kritische 'controleurs' van de ICT-ambities van de overheid ontwikkeld. Vanuit de eigen taakopdracht en met het eigen instrumentarium en bevoegdheden, beïnvloeden ze de ontwikkeling, richting en verdere uitbouw van de eOverheid. Een bijzondere positie als controleur komt toe aan 'de' burger zelf, die de ontwikkeling van de eOverheid op velerlei manieren controleert. Bovendien heeft technologie de aard van deze controlemogelijkheden de laatste jaren ingrijpend gewijzigd. Hoewel de burger geen institutie is – de processen die worden bekeken zijn allemaal spontaan van karakter –, kan wel worden gezegd dat het rolpatroon van burgers institutioneel is ingekaderd. In de eOverheid liggen onherroepelijk vooronderstellingen besloten ten aanzien van de rol van burgers: waar zij alert op dienen te zijn, hoeveel alertheid wordt gevergd, waartegen zij op kunnen komen en hoe.

7.1 BESTAANDE CONTROLE-INSTITUTIES

7.1.1 RAAD VAN STATE

De Raad van State toetst de uitbouw van de eOverheid vanuit zijn rol van wetgevingsadviseur. Behalve een analyse van de juridische houdbaarheid van het wetsvoorstel dat ten grondslag ligt aan een ambitie om technologie of informatie te benutten, vindt ook een beleidsanalytische toets en een beoordeling van de wetstechnische kwaliteit van het wetsvoorstel plaats. Omdat de regering de adviezen niet behoeft op te volgen, is de Raad van State uiteindelijk afhankelijk van diegenen tot wie de adviezen zijn gericht, de kwaliteit van hun antwoorden en – wanneer de adviezen niet worden opgevolgd – een gedegen argumentatie van de regering (Raad van State 2010: 127). Bij veel van de wetsvoorstellen op het terrein van ICT staat de juridische en wetstechnische toets in het teken van de grondrechten, het Europees Verdrag voor de Rechten van de Mens (EVRM) en de Wet bescherming persoonsgegevens (Wbp). Vanuit deze toets werd de regering onder

meer gevraagd de noodzaak en evenredigheid van de voorgenomen verwerking van bijzondere persoonsgegevens van bijna drie miljoen zorgverzekerden ten behoeve van de uitvoering van het wetsvoorstel tegemoetkoming chronisch zieken en gehandicapten alsnog dragend te motiveren (Raad van State 2009: 111). Op basis van de beleidsanalytische toets van het wetsvoorstel kilometerbeprijzing toonde de Raad van State zich kritisch over het technovertrouwen van de overheid dat sprak uit het registratie- en betalingssysteem dat de regering voor ogen stond. In het voorstel was er sprake van dat burgers het aantal kilometers dat door het 'kastje' was geregistreerd, niet aan konden vechten. De Raad van State gaf aan het vertrouwen van het kabinet in de techniek niet te delen (Raad van State 2010: 159).

Algemeen geconcludeerd, heeft de Raad van State zich vanuit zijn wetgevingstoetsende rol bij herhaling kritisch uitgelaten over de plannen van de regering om ICT in te zetten. Nut en noodzaak van de beoogde gegevensverwerking in de initiatieven van de regering staan niet altijd vast op het moment dat wetsvoorstellen bij de Raad van State voorliggen, aldus het Jaarverslag over 2008 (Raad van State 2009: 97). Toch blijkt het voor de Raad van State niet altijd eenvoudig de complexe problematiek in z'n volle omvang en op te verwachten effecten scherp te analyseren, te duiden en daarmee te toetsen. Leden van de Raad van State gaven in een gesprek met de WRR dan ook aan achteraf vast te moeten stellen het dossier over biometrie op het paspoort onvoldoende scherp getoetst te hebben.[1] Bovendien is de Raad van State bij zowel de wetstechnische als beleidsanalytische toets gebonden aan het instrumentarium dat hem ter beschikking staat. Men is gebonden door het toepasselijk wettelijk regime waaraan getoetst moet worden (bij veel ICT-gerelateerde initiatieven, de Wbp) en de individuele (beleids)context van het wetsvoorstel. Dat betekent dat het voor de Raad van State niet of nauwelijks mogelijk is in toetsende zin te anticiperen op de bredere context waarin het systeem zal (gaan) functioneren, zoals toekomstige koppelingen met andere applicaties waaruit nieuwe informatiestromen resulteren.

7.1.2 COLLEGE BESCHERMING PERSOONSGEGEVENS

Het College Bescherming Persoonsgegevens (CBP), dat toeziet op de rechtmatige verwerking van persoonsgegevens, heeft een breed takenpakket. Zowel advisering over wetgeving, klachtenbehandeling, ambtshalve onderzoek, bemiddeling bij geschillen over inzage en correctie, en sanctietoepassing behoren tot de taken van het College. Conform de Europese Privacyrichtlijn werkt het CBP samen met toezichthouders uit andere lidstaten en participeert het in de zogenaamde Artikel 29 Werkgroep die optreedt als adviseur van de Europese Commissie. De beperkt beschikbare capaciteit en middelen noodzaken het CBP tot selectiviteit, waardoor momenteel prioriteit wordt gegeven aan wetgevingsadvisering en handhaving. Op zowel deze prioriteitsstelling als de combinatie van functies binnen één organisatie is van diverse kanten kritiek geuit, zowel binnen als buiten de overheid (zie

hierover: Zwenne et al. 2007). Vanuit het perspectief van de organisaties waarop extern toezicht wordt uitgeoefend is het merkwaardig "dat zij zich voor voorlichting en advisering moeten wenden tot dezelfde instantie die hen later een tik op de vingers kan geven met behulp van ten behoeve van advisering verstrekte informatie" (commissie-Brouwer-Korf 2009). De commissie-Brouwer-Korf kwam daarom met de aanbeveling de toezichthouder geen bemoeienis te laten hebben met advisering, voorlichting of facilitering. Het CBP reageerde kritisch: het meent dat advisering over wet- en regelgeving hand in hand kan en moét gaan met de toezichthoudende taak (CBP 2010c).

Kijkend naar de eerste van de twee geprioriteerde taken, wetgevingsadvisering, stelt het College dat het aantal adviezen de laatste jaren min of meer gelijk is gebleven (CBP 2010c: 57). Uit de verschillende jaarverslagen valt op te maken dat het schommelt tussen de 38 (in zowel 2009 als 2010a) en 47 (2008). Wat opvalt bij de verschillende wetgevingstrajecten waarbij digitalisering aan de orde was, is dat het CBP uitdrukkelijk in de fase van de totstandkoming van wetgeving wordt betrokken, maar lopende het wetgevingstraject veelal niet meer in beeld komt. En dat terwijl latere amendementen op het wetsvoorstel de verwerking van persoonsgegevens soms overduidelijk raken. Illustratief is het criterium etniciteit in de Verwijsindex Risicojongeren, opgenomen nadat daarom in de Tweede Kamer bij motie was verzocht: de minister liet het parlement weten dat het CBP hierover niet geraadpleegd behoefde te worden (Prins 2010b). Treffend is ook het antwoord van de staatssecretaris van Binnenlandse Zaken op de vraag vanuit het parlement waarom het voorstel biometrie op het paspoort niet opnieuw aan het CBP was voorgelegd.

"Dat is omdat wij vonden dat wij zijn ingegaan op het [*sic*] kritiek van het CBP. Wij hebben een nadere onderbouwing gegeven. (...) Wij hebben de belangenafweging duidelijk gemaakt. Ik heb die nog eens uitgebreid toegelicht. Ik vind het een goede afweging. De Kamer moet het zelf wegen, maar wij hebben wel degelijk serieus aandacht besteed aan datgene wat het CBP heeft ingebracht. Ik vind het ook niet nodig om dan nog een keer langs een adviesorgaan te gaan. Dat doen wij ook niet bij de Raad van State. Wij schrijven een nader rapport dat de Kamer moet beoordelen. Die procedure hebben wij met elkaar afgesproken, want anders kunnen wij voortdurend bij adviesorganen langs blijven gaan. Dat lijkt mij niet de bedoeling (...)" (Eerste Kamer 2008-2009b; Böhre 2010: 81).

Het CBP had in een eerder stadium fundamentele kritiek op het wetsvoorstel en had de regering verzocht om een analyse van de voor- en nadelen van een centrale reisdocumentenadministratie. De regering gaf hier gevolg aan door de memorie van toelichting op enkele plaatsen aan te vullen, voornamelijk door in de tekst de voor- en nadelen van een centrale reisdocumentenadministratie op te noemen. De fundamentele bezwaren van het CBP (*function creep*, risico van misbruik, onjuist en onvoorzien gebruik) werden in één pagina van de memorie van toelich-

ting afgedaan. De overige bezwaren van het CBP (over inherente technische en beveiligingsrisico's) liet de memorie vrijwel geheel onbenoemd. Wel erkende de staatssecretaris dat "de in een databank opgeslagen vingerafdrukken en foto's die verband houden met een gestolen identiteitsdocument (…) de werkelijke eigenaar van die identiteit onophoudelijk grote problemen [kunnen] bezorgen. Biometrische gegevens zijn per definitie niet geheim en kunnen sporen achterlaten waardoor die gegevens verzameld kunnen worden zonder dat de eigenaar zich daarvan bewust is" (Tweede Kamer 2007-2008a: 23).

De tweede kerntaak van het CBP is handhaving. Recentelijk werden vanuit deze taak onder meer de beveiliging van ziekenhuissystemen, het bewaren door OV-bedrijven van de gegevens van het in- en uitchecken met de Studenten OV-chipkaart en de toepassing van automatische kentekenherkenning (ANPR) onder de loep genomen. Bij afwezigheid van onderzoek daarnaar is het niet eenvoudig vast te stellen in hoeverre het handhavend optreden door het CBP effect sorteert. Wel is duidelijk dat een handhavingsactie van het CBP soms voor de minister aanleiding is de gewraakte handelingen alsnog toe te staan door nieuwe wetgeving af te kondigen. Dat gebeurde begin 2010 toen de toezichthouder concludeerde dat het bewaren van ANPR-gegevens die geen hit opleverden in strijd was met de wet. De ministers van Binnenlandse Zaken en Justitie kondigden daags hierna plannen aan voor een wettelijk kader dat deze mogelijkheid wel zou legitimeren (Tweede Kamer 2009-2010f). Maar ook andere signalen laten zien dat een doelmatige en effectieve handhaving door het College verre van eenvoudig is. Zo lijkt het CBP de diversiteit aan toepassingen die op lokaal en regionaal niveau vorm en inhoud krijgen lang niet altijd scherp in het vizier te hebben. Handhaving strekt zich dan ook niet of nauwelijks tot dat niveau uit, waardoor lokale ambities ogenschijnlijk zonder enige rem, sturing of controle gerealiseerd lijken te kunnen worden (Keymolen & Prins 2011). Bovendien, zo is hiervoor uiteengezet, reiken juist op uitvoeringsniveau de gegevensprocessen over de grenzen van sectoren heen, terwijl bij het CBP nog een sectorsgewijze benadering van kansen en risico's centraal staat. In 2004 merkt het CBP daarover in de zelfevaluatie op dat deze methode aansluit bij aard en functie van het toezicht (CBP 2004). Bovendien blijken beide door het College geprioriteerde rollen – handhaving en wetgevingsadvisering – soms een bepaalde politieke dynamiek te krijgen, die door het College zelf niet te sturen is. De geschiedenis van het Elektronisch Patiëntendossier is hierin illustratief. De minister van VWS maakte dankbaar gebruik van het zeer kritische rapport dat het CBP publiceerde over de beveiliging van ziekenhuissystemen. De door het CBP gesignaleerde problemen bij de lokale systemen waren voor de minister een extra argument om het belang van het landelijk systeem van het EPD te benadrukken (Eerste Kamer 2009-2010c). Door dit betoog van de minister vervolgens niet expliciet tegen te (kunnen) spreken, leek het CBP impliciet steun te geven aan het EPD, althans de voorkeur te geven aan een landelijke aanpak boven een regionale. Problematisch in dit verband is dat de inhoudelijke bevindingen van

het CBP over de beveiliging van de ziekenhuissystemen niet openbaar zijn en daarmee ook niet af te zetten zijn tegen de beoogde beveiligingsgaranties die voor het landelijke systeem zijn voorzien.

De nadruk op handhaving en wetgevingsadvisering betekent dat er geen plaats meer is voor advisering op maat door het College en er een verschuiving heeft plaatsgevonden naar controles *ex post* in plaats van *ex ante* (CBP 2010c: 36). Burgers kunnen hun klachten weliswaar melden via de (nogal statische) website mijnprivacy.nl, maar hun individuele klacht zal niet in behandeling worden genomen. Bedrijven en publieke organisaties kunnen er met hun vraag om advies niet terecht. Het CBP richt zich expliciet niet op een interactie met individuele verwerkers en burgers, bijvoorbeeld in de vorm van gebruikers- of adviesraden of consultatierondes, ondanks aansporingen om die kant wel op te gaan (Ambtelijke Commissie Toezicht II 2004: 15-16). In het Verenigd Koninkrijk bijvoorbeeld consulteert de toezichthouder wel (Information Commissioner's Office 2007).

7.1.3 NATIONALE OMBUDSMAN

Ook de Nationale Ombudsman toetst de ontwikkeling van de eOverheid. Dat doet hij door, in een klachtenprocedure of uit eigen beweging, een oordeel te vellen over de behoorlijkheid van het overheidsoptreden. Onder de behoorlijkheidsvereisten vallen naar de invulling van de Nationale Ombudsman, de grondrechten, materiële behoorlijkheid (evenredigheid, gelijkheid en rechtszekerheid), formele behoorlijkheid (motivering en fair play) en de instructienormen van zorgvuldigheid (professionaliteit, informatieverstrekking en administratieve nauwkeurigheid). Een bestuursorgaan is niet gehouden om aan het oordeel van de Nationale Ombudsman gevolgtrekkingen te verbinden.

Waar burgers met hun individuele klachten geen gehoor vinden bij het CBP, is dat wel het geval bij de Nationale Ombudsman. De verschillende jaarverslagen tonen een variëteit aan klachten en daaropvolgende interventies: van de in de media breed besproken zaken over identiteitsfraude in de politieketen en andere systemen van de overheid, via de gegevensverwerking in IND-systemen, de OV-chipkaart voor studenten (waar bleek dat de IB-Groep in feite de macht om een directe oplossing te bieden uit handen had gegeven aan de OV-bedrijven) en de plaatsing van foto's van een onterecht verdachte op de politiewebsite overvallers.nl tot de problemen met de ketensamenwerking tussen de Belastingdienst, de Sociale Verzekeringsbank, pensioenfondsen en het Uitvoeringsinstituut Werknemersverzekeringen (UWV) ten behoeve van de uitvoeringstaken van het College voor Zorgverzekeringen, enzovoorts (Nationale Ombudsman: 2009). Ondanks het rijke beeld dat uit de jaarverslagen opdoemt over de problemen waar burgers zoal tegenaan lopen als de overheid ICT inzet, blijft het primair een beeld per overheidsinstelling. Alhoewel de Nationale Ombudsman in de recente jaarverslagen

uitdrukkelijk aandacht besteedt aan problemen die voortkomen uit het werken in ketens, blijkt het nauwelijks mogelijk een scherp inzicht te krijgen in de omvang, ernst en kenmerken van de klachten die specifiek verband houden met de inzet van ICT. Meer algemeen blijkt het verre van eenvoudig om vanuit de dossiers die over de jaren zijn opgebouwd bij niet alleen de Nationale Ombudsman, maar ook het CBP en meer recent het Meldpunt Identiteitsfraude, inzicht te krijgen in de problemen waar burgers voor staan. Ook de instanties zelf blijken het beeld in feite niet paraat te hebben. Choenni et al. (2011) laten in hun analyse zien dat de registraties bij al deze instanties niet direct dan wel slecht te relateren zijn aan de rol die ICT heeft gespeeld bij klachten van burgers.

7.1.4 ALGEMENE REKENKAMER

De Algemene Rekenkamer heeft als opdracht te controleren of de inkomsten en uitgaven van de overheid (het rijk) kloppen, of het vastgestelde beleid wordt uitgevoerd en of het werkt zoals het beoogd was. Zoals in eerdere hoofdstukken opgemerkt, is dit een belangrijke rol in het licht van de *drive* van de eOverheid. De Rekenkamer toetst immers of de beloofde verbeteringen in effectiviteit en efficiëntie van beleid daadwerkelijk uitkomen. Het is aan de regering en/of het parlement om consequenties aan de conclusies van de Rekenkamer te verbinden en er politieke uitspraken over te doen.

De Algemene Rekenkamer heeft zich, zoals in eerdere hoofdstukken opgemerkt, de afgelopen jaren kritisch tot zeer kritisch uitgelaten over zowel de ICT-projecten als de informatiehuishouding bij de overheid. Waar controle op de inkomsten en uitgaven van de ICT-projecten voor de Rekenkamer nog een redelijk hanteerbare (want redelijk te kwantificeren) klus is, ligt dat veel minder eenvoudig bij de beoordelingen van de informatiehuishouding van de overheid. Toch oordeelt de Rekenkamer ook op dit dossier al jarenlang kritisch. Er is sprake van een gebrekkige aandacht voor het informatiebeheer, dat de Rekenkamer mede verklaart door het feit dat bij de overheid "de informatiehuishouding 'slechts' ondersteunend is aan het bedrijfsproces. Dit in tegenstelling tot de situatie in bedrijven" (Algemene Rekenkamer 2009: 8). Echter, een duurzame informatiehuishouding zal "zonder voortdurende aandacht en vasthoudendheid van de ambtelijke en politieke leiding van de departementen hoogstwaarschijnlijk niet tot stand komen" (Algemene Rekenkamer 2009: 8). Problemen worden nu nog te vaak afgedaan als incidenten en met een eenmalige actie opgelost, totdat er zich een nieuw probleem aandient en men weer opnieuw aan de slag moet. Van de overheid mag worden verwacht dat ze een visie ontwikkelt op hoe om te gaan met de snelle veranderingen die de digitalisering van informatie met zich meebrengt, aldus de Rekenkamer. Zo is er aandacht nodig voor de archivering van digitale informatie als e-mail, sms en twitter. Bij het (eerste) gebruik van informatie moet al nagedacht worden over de wijze van archivering en vindbaarheid, en onderzocht in welke mate de informatie van

belang is voor het erfgoed (Algemene Rekenkamer 2010b). Daarbij stelt men terzijde ook vast dat eigen onderzoek in het buitenland geen aansprekende *good practices* oplevert die passen binnen het Nederlandse bestuurlijke klimaat (Algemene Rekenkamer 2009: 21). Overigens vraagt de Rekenkamer al veel langer en met regelmaat om een beleidsvisie en kader voor de archivering, vernietiging en bewaring van digitale bestanden (Algemene Rekenkamer 1991; Algemene Rekenkamer 1998). De Rekenkamer staat niet alleen. Ook het rapport *Een dementerende overheid* van de Rijksarchiefinspectie uit 2005 en het rapport van de Raad voor Cultuur en de Raad voor het openbaar bestuur (2008) zijn alarmerend van toon. De inspectie stelt vast dat overheidsorganisaties vaak geen overzicht hebben van de plaatsen waar zij hun digitale bedrijfsvoering- en verantwoordingsinformatie bewaren. Er zal op hoog bestuurlijk niveau veel actiever gestuurd moeten worden op de informatiehuishouding (Rijksarchiefinspectie 2005). Het kabinet onderschrijft in diverse reacties de conclusies van de rapporten. De noodzaak van zowel visievorming, een integrale benadering als cultuurverandering wordt onderkend (Tweede Kamer 2008-2009e). Niet alleen neemt de hoeveelheid informatie explosief toe, ook de verschillende verschijningsvormen volgen elkaar in rap tempo op. Een visie op archivering en digitale duurzaamheid ijlt daar vrijwel onvermijdelijk steeds achteraan. Daarom is het cruciaal dat de overheid greep krijgt, juist op de dynamiek van het vraagstuk van archivering en digitalisering. Vanuit het belang van bedrijfsvoering, verantwoording en cultureel erfgoed is het wenselijk om al aan de 'voorkant' van de informatieketen na te denken over duurzaamheid, aldus het kabinet (Tweede Kamer 2005-2006b: par. 3.2). In een gesprek met de WRR benadrukte de president van de Rekenkamer Stuiveling dat het echter om veel meer gaat dan het verleggen van de focus naar de voorkant van de informatieketen. Langzamerhand worden de grenzen aan de 'maakbaarheid' van het digitale archief duidelijk. Misschien moeten we ons erbij neerleggen dat een archief organisch groeit en moeten we ons vooral richten op zoekstrategieën. Het is belangrijk om nieuwe manieren te verzinnen om informatie die we gedacht hadden nooit meer nodig te hebben, later toch nog terug te vinden. Er zal binnen de overheid gewerkt moeten worden aan een cultuuromslag als het om gedigitaliseerde informatieprocessen gaat: niet langer vanuit een klassiek lineaire focus op creatie, gebruik, beheer en archivering maar als gelijktijdig proces waarbij de verschillende waarden van informatie (bedrijfsproces, institutioneel geheugen, cultureel erfgoed, verantwoording, recht- en bewijszoekenden) gelijkwaardig en in samenhang gelden. Hiervoor zal de bureaucratie meer als een open systeem moeten gaan werken.

7.1.5 rechterlijke macht

Waar het bestuur zich formeel niets gelegen hoeft te laten liggen aan het oordeel van alle hiervoor genoemde instanties, heeft ze zich uiteindelijk wel wat aan te trekken van de uitspraak van de rechter. Maar waar burgers met hun klachten over

de digitalisering van de overheid wel aankloppen bij de Nationale Ombudsman en in beperkte mate bij het CBP, doen ze dat nauwelijks bij een rechterlijke instantie. Overigens doet dit verschijnsel zich ook in andere landen voor (Mayer-Schönberger 2009: 138-139). Kennelijk is een zelfstandig actierecht over informatie moeilijk 'op gang te brengen': burgers komen op tegen hun onwelgevallige beslissingen, maar hebben niet in de gaten dat ze ook een 'informatiegeschil' kunnen hebben. Zo concludeerden de evaluatierapporten van de Wet bescherming persoonsgegevens (Wbp) dat het aantal rechterlijke uitspraken over de Wbp zeer beperkt is (Zwenne et al. 2007; Winter et al. 2008). Deze constatering kan worden doorgetrokken naar andere wetgeving die de omgang met persoonsgegevens regelt, zoals de Wet politiegegevens, de Wet GBA, enzovoorts. Rechters hebben, kortom, weinig kunnen bijdragen aan de interpretatie en handhaving van regels voor de gedigitaliseerde verwerking van persoonsgegevens. Spaarzame uitzonderingen zijn de uitspraak van het Hof Leeuwarden, juni 2010,[2] waarin werd geconcludeerd dat de wettelijke basis ontbreekt voor het gebruik van beelden van registratiecamera's boven een snelweg voor een opsporingsonderzoek en de uitspraak van de Hoge Raad, maart 2010, over de vordering van gegevens door het Openbaar Ministerie bij Trans Link Systems (Buruma 2011). Er waren ten behoeve van een stafrechtelijk onderzoek NAW-gegevens en pasfoto's gevorderd van alle reizigers die met een persoonsgebonden OV-chipkaart op een bepaald tijdstip op bepaalde metrostations in Rotterdam aanwezig waren. De Hoge Raad bepaalde dat de pasfoto's uitsluitend mogen worden opgevraagd na machtiging van de rechter-commissaris en slechts onder die voorwaarde mogen worden gebruikt in een strafrechtelijk onderzoek.[3]

Op terreinen waar burgers financieel worden geraakt is het beeld enigszins anders. Illustratief zijn bijvoorbeeld de rechtszaken over fouten in de systemen van de Belastingdienst of de uitwisseling van gegevens met een voor de aanslagregeling ingeschakelde (externe) organisatie (Gribnau 2010). Deze laatste situatie stond centraal in een procedure uit 2009. Door een systeemfout waren onjuiste gegevens uitgewisseld tussen de gemeentelijke basisadministratie en Cocensus, het bedrijf aan wie de betreffende gemeente de belastingheffing voor afvalstoffen had uitbesteed. De gemeente trachtte het gemiste bedrag alsnog bij de burger te verhalen. De rechter oordeelde echter dat navordering niet mogelijk was.[4] Maar evenals bij de uitspraak van het CBP over automatische kentekenherkenning toont de regering zich ook hier soms een slecht verliezer en reageert ze daags na het negatieve oordeel vanuit de rechterlijke macht met de aankondiging van reparatiewetgeving om de situatie naar de eigen hand te zetten. Illustratief is de reactie van de minister van Financiën op het oordeel van de Hoge Raad dat een navordering niet mogelijk was bij een onjuiste aanslag ten gevolge van een fout in het ontwerp van het geautomatiseerde systeem.[5] De minister presenteerde een wetsvoorstel om navordering bij grote missers bij het gebruik van ICT mogelijk te maken (Tweede Kamer 2009-2010h).

Zeker in vergelijking met andere landen krijgt de rechterlijke macht in ons land weinig gelegenheid zich over de ICT-ambities van de overheid uit te spreken. In een brief aan de Eerste Kamer suggereert de minister van Justitie dat het ontbreken van "een zekere georganiseerde beweging met enige aanspraak op representativiteit van burgers die specifiek opkomen voor de bescherming van hun gegevens" van invloed is op de mate waarin geschillen over het gebruik van gegevens aan de rechter worden voorgelegd (Eerste Kamer 2009-2010a: 48). Een mogelijk belangrijker argument lijkt te zijn dat ons land (vooralsnog) niet de mogelijkheid tot toetsing aan de Grondwet kent. Uitspraken in niet alleen Duitsland (zoals die over dataretentie van 2 maart 2010[6]), maar eerder al in Roemenië (8 oktober 2009[7]) laten zien dat wetgeving die het de overheid toestaat gegevens te verwerken met een zekere regelmaat door constitutionele rechters ongedaan wordt gemaakt. Overigens zijn de internationale gerechten, in het bijzonder het Europees Hof voor de Rechten van de Mens, wel in staat geweest een duidelijke lijn neer te zetten (De Hert 2011). Die lijn is kritisch ten aanzien van de ambities en komt er kort geformuleerd op neer dat lidstaten duidelijk maat moeten weten te houden als ze technologie inzetten voor het verzamelen en verwerken van persoonsgegevens (De Hert 2009).

7.1.6 NIEUWE ARRANGEMENTEN

In aanvulling op de Algemene Rekenkamer, de Raad van State, Nationale Ombudsman, het CBP en/of de rechterlijke macht hebben ook andere actoren en instanties de afgelopen jaren een rol gekregen en opgepakt bij toezicht, controle en verantwoording. Zo hebben de eerdergenoemde CIO's een rol gekregen bij het tijdig en adequaat informeren van het parlement om diens taak als controlerende macht te faciliteren. En in het regeerakkoord van het kabinet-Rutte is afgesproken dat er een nationale toezichthouder komt voor datalekken: "Het kabinet komt met een voorstel voor een meldplicht voor alle diensten van de informatiemaatschappij, waaronder de overheid, in geval van verlies, diefstal of misbruik van persoonsgegevens waarbij alle datalekken worden gemeld aan de nationale toezichthouder die boetes kan opleggen indien de meldplicht niet wordt nageleefd" (Regeerakkoord 2010: 42). In het Verenigd Koninkrijk is specifiek met het oog op identiteitsmanagement een toezichthouder voor identiteitsmanagement aangesteld, namelijk de Identity Commissioner. Hij moet onder meer toezien op naleving van de Identity Cards Act uit 2006. De huidige Britse regering heeft inmiddels aangekondigd om de National ID Card, en daarmee ook de functie van Identity Commissioner, te schrappen.

Behalve nieuwe instituties zijn er ook nieuwe arrangementen. Met name de verschillende uitvoeringsinstanties initieerden eigen arrangementen voor *checks and balances*. Overigens is deze ontwikkeling al langer zichtbaar, maar de inzet van ICT heeft hier duidelijk stimulerend gewerkt. Dit vindt zijn oorsprong niet

alleen in de nieuwe instrumenten die zich met de komst van een technologie aandienen, maar zeker ook als reactie op de specifieke complexiteit en veranderende verhoudingen die de inzet van ICT met zich meebrengt. Illustratief zijn de cliëntraden en klantenpanels die worden ingezet door onder meer de SVB en het UWV om burgers te laten meepraten over en feedback te geven op online initiatieven (bijvoorbeeld het Digitaal Verzekeringsbericht of via www.burgerpolis.nl). Gewezen kan ook worden op de instrumenten (Gateway Review en IT-Dashboard) die het parlement beogen te voorzien van actuelere rapportages over de voortgang van (grote) ICT-projecten (Snijders 2011). Verder vormen de online meldpunten zoals het Meldpunt Identiteitsfraude en Meldpunt Burgerservicenummer (BSN) een illustratie van nieuwe arrangementen voor toezicht en controle. Volgens Nationale Ombudsman Brenninkmeijer blijkt juist de aanwezigheid van de menselijke factor een belangrijk element bij het succes van een aantal van de genoemde arrangementen. Kwaliteit en integriteit van systemen zijn erg afhankelijk van organiseren van menselijke feedback, feedbackloops en terugkoppeling aan burgers, bijvoorbeeld via de zogenaamde Stella-teams van de Belastingdienst.[8]

Een instrument dat meer recent aan populariteit wint zijn de zogenaamde Privacy Enhancing Technologies (PETs). In feite wordt het toezicht op en de handhaving van de wettelijke regels voor de omgang met persoonsgegevens in handen van de technologie gelegd. Opvallend is dat de regering al op 18 november 1999 via de motie Nicolai kamerbreed werd opgeroepen in de systemen van de overheid PET toe te passen (Tweede Kamer 1999-2000). Tot op heden is daar door de overheid nauwelijks gehoor aan gegeven. Toen het ministerie van BZK in 2003 bij zeven overheidsinstanties aanklopte om proefprojecten op te zetten, werd vanuit deze instanties aangegeven dat men het niet opportuun achtte met PET aan de slag te gaan (Borking 2010). Een in datzelfde jaar in opdracht van BZK door Research and Development Corporation (RAND) Europe uitgevoerd onderzoek noemt vijf argumenten voor het gebrek aan animo binnen de overheid voor PET: de bestaande methoden van privacybescherming voldoen; privacybescherming is niet nodig; experimenten met PET zijn een gevaar voor de betrouwbaarheid, kwaliteit van de dienstverlening en het imago van de overheidsinstantie; PET is nog niet volwassen en er is geen tijd, geld of mankracht om de invoering van PET te realiseren (Borking, 2010). Drie jaar later stelde de evaluatie van de Wet persoonsgegevens vast dat de houding in feite niet was veranderd (Zwenne et al. 2007). Maar inmiddels lijkt het klimaat gunstiger: zowel op het internationale (de Werkgroep 29 voor de bescherming van persoonsgegevens van de Europese Commissie en de European Data Protection Authority – EDPS) als op het nationale (kabinet, parlement en CBP) niveau klinkt de roep om nu serieus werk te maken van PET luid en duidelijk.

7.2 De veelzijdige burger

In de ruime zin van het woord bevinden toezichthouders zich natuurlijk ook buiten de overheid. Dat geldt in de eerste plaats voor de media die ontwikkelingen en initiatieven bij de eOverheid kritisch volgen, zoals op vele plaatsen in dit rapport is terug te vinden. Een groeiend aantal burgerinitiatieven en vertegenwoordigers van burgers en consumenten stelt zich op als luis in de pels en dwingt de overheid bij regelmaat tot het (beter) afleggen van verantwoording voor dan wel bijstellen van de plannen en ambities. Naar aanleiding van de campagne van de actiegroep "wij vertrouwen stemcomputers niet" besloot het kabinet in 2007 zelfs tot het stopzetten van het gebruik van stemcomputers. Soms zijn burgers professioneel en formeel georganiseerd – in bijvoorbeeld de Consumentenbond – en soms betreft het losse, ad-hocverbanden van burgers. De wijze waarop burgerinitiatieven daarbij ICT inzetten heeft de 'mobilisatie van meningen' ingrijpend veranderd. De razendsnelle verspreiding van informatie die door ICT en sociale media mogelijk wordt gemaakt, kan een beleidsvoornemen in de kiem smoren dan wel ter discussie stellen (denk aan de vaccinatie voor baarmoederhalskanker) of een politieke discussie doen kantelen (zoals de hierna te bespreken ontwikkelingen rondom het biometrisch paspoort laat zien). De veranderende houding van burgers ten opzichte van de overheid lijkt er, wat betreft de inzet van ICT door de overheid, steeds meer een van toegenomen activisme. Deze actieve burgers richten zich daarbij niet uitsluitend op het controleren van de overheid en gaan soms heel anders te werk dan de 'traditionele' toezichthouders. Hoewel burgerinitiatieven dikwijls een controlerende en corrigerende functie kennen, gaan sommige van de initiatieven nog een stapje verder. Burgers nemen, gefaciliteerd door sociale media, uit onvrede overheidstaken over of gaan zelf aan de slag om de overheid transparanter (en bijgevolg beter controleerbaar) te maken. Desalniettemin blijft het voor (individuele) burgers nog steeds lang niet eenvoudig om tijdig in het proces 'mee te praten' en 'mee te denken' over de digitaliseringsinitiatieven. Zelden bijvoorbeeld worden burgers in de beleidsvoorbereidende fase via een openbare consultatie uitgenodigd hun inbreng te leveren.

7.2.1 Beïnvloeden van beleid

Illustratief als het gaat om het beïnvloeden van beleid is het eerdergenoemde wetsvoorstel voor de introductie van de slimme energiemeter dat in april 2009 in de Eerste Kamer strandde. Nadat de Consumentenbond bij de senatoren had aangeklopt met een zeer kritische boodschap over onder meer de privacyimplicaties van het initiatief (Eerste Kamer 2008-2009a) en er door burgers via onder meer de website wijvertrouwenslimmemetersniet.nl actie was gevoerd, bleek de minister genoodzaakt het wetsvoorstel aan te passen. Het gebruik van door de energiemeters gegenereerde gegevens – met uitzondering van enkele basisgegevens benodigd voor de facturering – werd in dit nieuwe voorstel uitsluitend nog

op basis van toestemming van de eindgebruiker toegestaan (Tweede Kamer 2009-2010e). In het oorspronkelijke voorstel had de eindgebruiker niets over het gebruik van de gegevens te zeggen.

7.2.2 ZELF HET HEFT IN HANDEN

Niet altijd is een burgerinitiatief erop gericht het beleid bij te sturen. Uit onvrede kunnen burgers ook taken die van oudsher bij de overheid liggen zelf gaan uitvoeren. Een bekend voorbeeld van digitale eigenrichting van burgers is de site stopkindersexnu.nl en zijn opvolgers, die telkens worden gelanceerd als de overheid maatregelen neemt tegen het bestaande internetadres. Via dit kanaal worden de (woon)gegevens van eerder veroordeelde, maar nu reïntegrerende pedoseksuelen gepubliceerd. De burgers (ouders) die deze toepassing produceren, consumeren, en er op uiteenlopende manieren naar handelen, hebben inderdaad alle belang bij de wetenschap dat een dergelijk figuur in de straat komt wonen, maar de zo gevestigde ‘spontane justitie’ ondergraaft het uitgangspunt dat de wet en de overheid hanteren, namelijk dat iedere overtreder weer een plek in de maatschappij moet kunnen krijgen. Een speelsere variant van het ondergraven van de overheidshandhaving is de site flitsservice.nl, waarop onder meer de locaties van flitspalen en mobiele flitsers (bijv. ingebouwd in Kliko’s) voortdurend worden bijgehouden.

7.2.3 MEER TRANSPARANTIE

Naast initiatieven gericht op het veranderen van beleid of het zelf uitvoeren van overheidstaken zijn er ook burgers die zich inspannen voor meer overheidstransparantie. Zo trachten organisaties als Stichting Het Nieuwe Stemmen en andere initiatieven transparantie en participatie via internet te versterken, of dat nu tot doel heeft een beter geïnformeerd stemgedrag (wiekiesjij.nl), de versterking van het recht van petitie en burgerinitiatief (petities.nl) of het verlagen van de drempel om politici te benaderen (maildepolitiek.nl). Illustratief is ook de oprichting van de Stichting Kritische IT Infrastructuur. Dit initiatief vestigt de aandacht op de noodzaak van een fundamentele discussie over de rol van politiek-maatschappelijke en bestuurlijke overwegingen bij de selectie van systemen, software en ICT-uitbestedingen door de publieke sector. Tot de categorie ‘geïnstitutionaliseerde tegenkrachten’ behoort ook de werking van de Wet openbaarheid van bestuur, die recentelijk is versterkt met een *tool* die zogenaamde Wob-verzoeken voor gewone burgers (niet-journalisten) binnen bereik brengt (woberator.nl). Hoewel vandaag de dag vele malen meer informatie vrijgegeven wordt door de overheid dan in het verleden het geval was, levert deze transparantie vanuit de overheid slechts informatieproducten op die al *processed* zijn: de overheid heeft al (beleids)informatie van de werkelijkheid gemaakt. Ingrijpender zijn daarom de ‘open data’-initiatieven, die bijvoorbeeld in het Verenigd Koninkrijk plaatsvinden. Het gaat hier om ruwe overheidsdata in plaats van om overheidsinformatie. De

burger kan zo echt inzicht krijgen in de keuzes die de overheid maakt op grond van de data die haar ter beschikking staan. Maar daarnaast kan de burger ook creatief aan de slag met de vrijgegeven data, om daar nieuwe (publiek getinte) toepassingen voor te verzinnen, zoals verontreinigingskaarten, de Misdaadkaart (een kaart waarbij persberichten van de politie gecombineerd worden met locatiebepalingen), maar ook de BBC News map (een kaart waarop te zien is waar het nieuws waarover de BBC bericht zich afspeelt).

De invloed van deze verschillende burgerinitiatieven is terug te zien in de mate waarin de overheid zulke initiatieven omarmt en zich aansluit. Steeds vaker worden initiatieven van burgers ondersteund en/of geadopteerd. Zo zijn het programma Burgerlink van het ministerie van BZK en de site digitalepioniers.nl opgericht om burgerinitiatieven te adopteren. Voor de initiatiefnemers kan dat echter een dilemma opleveren tussen zich laten subsidiëren en de zelfstandigheid verliezen, of verder ploeteren zonder verdienmodel, op puur enthousiasme.

7.2.4 BURGERS EN HUN LEIDENDE BEGINSELEN

Burgerinitiatieven zijn steeds minder slechts een *countervailing power* in de marge. Burgerrechtenbewegingen werken samen met bekende internationale mensenrechtenorganisaties, organiseren zich razendsnel via nieuwe media, beschikken soms over flinke financiële middelen en gaan met deskundige ondersteuning, onder meer vanuit de advocatuur, 'de strijd' aan. Deze strijd kreeg onder meer momentum in de zomer van 2009, toen een brede coalitie van ngo's onder leiding van het Nederlands Juristen Comité voor de Mensenrechten (NJCM) de centrale opslag van biometrische gegevens onder de nieuwe Paspoortwet aanvocht bij het VN-Mensenrechtencomité.[9] Vervolgens werd de digitale burgerrechtenbeweging Bits of Freedom heropgericht en mengden ook organisaties als de Consumentenbond zich in het privacydebat. De discussie lijkt zich thans verder te professionaliseren en mogelijk te verharden. Stichting Privacy First – daarbij terzijde gestaan door een advocatenkantoor – begon in 2009 met de voorbereiding van een rechtszaak tegen de voor de Paspoortwet verantwoordelijk bewindspersoon. Eerder al had vereniging Vrijbit via een spoedprocedure bij het Europees Hof voor de Rechten van de Mens (EHRM) getracht de introductie van de nieuwe wet tegen te houden. Een andere organisatie (Het Nieuwe Rijk) verspreidde eind november 2009 een folder die de indruk wekte afkomstig te zijn van de overheid en die burgers opriep hun Burgerservicenummer in hun arm te laten tatoeëren. De verantwoordelijke staatssecretaris kondigde aan juridische stappen tegen de actie te ondernemen. Het Openbaar Ministerie liet op 11 januari 2010 echter weten de klacht van de staatssecretaris niet in behandeling te nemen. Maar een dag later achtte de Reclame Code Commissie zich wel bevoegd en oordeelde dat de 'reclame-uiting' in strijd was met de Nederlandse Reclame Code[10].

Alhoewel het kritische geluid vanuit de samenleving zich in de meerderheid van de gevallen richt op het verankerende beginsel van privacy – denk maar aan wijvertrouwenslimmemetersniet.nl en de actie van Het Nieuwe Rijk over het tatoeëren van het Burgerservicenummer – zijn er ook initiatieven die het belang van het procesmatige beginsel van transparantie aan de orde stellen. Zo wil de eerdergenoemde Stichting Kritische IT Infrastructuur dat de selectie van ICT-systemen door meer wordt bepaald dan uitsluitend operationele overwegingen, maar dat er ook aandacht is voor transparantie en democratische controleerbaarheid van applicaties en systemen en onafhankelijkheid van de overheid. In zekere zin presenteren al deze georganiseerde burgers zich als een nieuw soort toezichthouders en zien zij voor zichzelf een rol weggelegd als organisator van tegenkrachten om bepaalde ICT-initiatieven van de overheid aan de kaak te stellen, tegen te houden dan wel ongedaan te maken. Maar met hun komst en optreden als toezichthoudende en controlerende actor rijzen ook vragen. Vragen over de instrumenten die zij ter hand nemen en/of hun ter beschikking staan, hun rechtspositie en de dilemma's rondom de legitimiteit van hun optreden (in hoeverre spreken zij namens burgers, zijn de procedures die leiden tot het besluit tot een bepaalde actie transparant en controleerbaar, zijn de bronnen op basis waarvan zij handelen voldoende betrouwbaar, kenbaar en verifieerbaar, enz.).

7.3 CONCLUSIE

De consequenties van de eOverheid beginnen steeds zichtbaarder te worden. Daarmee begint het debat over de wenselijkheid daarvan en de richting die vervolgens moet worden ingeslagen meer en meer te leven, zo laat het toegenomen activisme althans zien. Niettemin wordt dit debat (nog) zeer door toeval bepaald. Het komt voor dat de maatschappelijke dynamiek die een bepaalde kwestie tot een 'heet hangijzer' maakt pas opkomt lang nadat de formele besluitvorming is afgerond. Het voorbeeld van biometrie op het paspoort toont dat er tussen politieke besluitvorming en accountability enerzijds en de ervaringen en gevoeligheden van burgers anderzijds een slechte aansluiting kan bestaan. Maar tegelijkertijd is de aandacht voor dit specifieke dossier vrij willekeurig: er zijn tal van dossiers waar een publieke discussie ook geen overbodige luxe zou zijn, maar waar die toch niet plaatsvindt. Voor de meeste zaken geldt dat 'de maatschappij' het oordeel over de ontwikkeling van de eOverheid in handen van het parlement (en de regering) en de indirect betrokken controleurs lijkt te leggen. Die staan daarmee voor de lastige taak om applicatie voor applicatie, koppeling voor koppeling te bepalen hoe de informatisering van de relatie overheid-burger vorm moet krijgen. Het blijkt daarbij voor deze controleurs verre van eenvoudig een duidelijk beeld te krijgen van de afwegingen die moeten worden gemaakt, en om die vervolgens daadwerkelijk te toetsen en van een eigen oordeel te vergezellen. De controleurs van de eOverheid zijn in hun taak en in hun aandacht ofwel beperkt tot het toetsen van de voorliggende applicatie zonder die in een bredere

context te (kunnen) bezien, ofwel beperkt tot een bepaald aspect van de ontwikkeling van eOverheid.

In dit hoofdstuk over de controleurs van de eOverheid ging het niet alleen over de totstandkoming van de (grote) beleidskeuzes – waarbij de Raad van State, de Algemene Rekenkamer, de Nationale Ombudsman en de 'digitale voorhoede' een rol vervullen –, maar ook over de vraag hoe transparantie en accountability voor individuele burgers zijn vormgegeven. Die vormgeving draait om de vraag naar de informatiepositie (transparantie) en de ingangen (accountability) van/voor burgers die in hun individuele belangen worden getroffen. In deze dimensie doen zich grote problemen voor, die scherp zijn neergezet door de Nationale Ombudsman, maar ten aanzien waarvan – opmerkelijk genoeg – noch het CBP noch de rechter zich echt laat gelden. Die problemen zijn eigenlijk als volgt samen te vatten: de ontwikkeling van de efficiënte maar evengoed klantgerichte eOverheid is niet gepaard gegaan met een versterking van het inzicht dat de burger kan krijgen in zijn of haar eigen (informatie)positie en de mogelijkheden om daarin corrigerend op te treden. Bij besturen in ketens en netwerken is geen organisatorisch ingebed systeem voor de bescherming van burgers in deze ketens en netwerken gevoegd. Die emancipatie van de informatie- en rechtspositie van burgers is aan de orde nu de eOverheid weliswaar voor de massa van beslissingen een vooruitgang behelst, maar voor een minderheid van gevallen waarin informatieprocessen mislopen een des te grotere kwetsbaarheid oplevert.

NOTEN

1 Gesprek met dhr. C.J.M. Schuyt, dhr. M. Oosting, dhr. M. Raijmakers, mevr. H.J.Th.M. van Roosmalen, Raad van State, april 2010.

2 LJN: BM8100.

3 LJN: BK6331, Hoge Raad, 08/04524 B.

4 Rechtbank Haarlem 11 september 2009, nr. 09/902, NTFR 2009/2158.

5 HR 14 maart 2008, nr. 43.301, NTFR 2008/551.

6 Bundesverfassungsgericht, 2 maart 2010, zaaknrs. 1 BvR 256/08, 1 BvR 263/08 & 1 BvR 586/08; raadpleegbaar op www.bundesverfassungsgericht.de.

7 Curtea Constitutional 8 oktober 2009, zaaknr. 1.258, http://www.ccr.ro/decisions/pdf/ro/2009/D1258_09.pdf, geraadpleegd op 18 november 2010.

8 Interview met dhr. A. Brenninkmeijer, Nationale Ombudsman, februari 2010.

9 Zie <http://www.njcm.nl/site/press_releases/show/25>; <http://www.binnenlandsbestuur.nl/nieuws/2009/07/protest-tegen-opslagvingerafdruk.121883.lynkx>.

10 Beslissing van de Reclame Code Commissie, Amsterdam 12 januari 2010: http://www.reclamecode.nl/consument/default.asp?nieuwsID=391&terugURL=%2Farchiefnieuwsberichten%2Easp%3FhID%3D7.

DEEL III

ANALYSE EN AANBEVELINGEN

8 DE iOVERHEID

De mogelijkheden die moderne ICT biedt zijn voor de overheid groot en verleidelijk. De belofte van snellere werkprocessen, grotere effectiviteit en efficiëntie van beleid, een betere en meer op maat gesneden dienstverlening en minder papieren bureaucratie behoren tot de aantrekkingskracht van de eOverheid. Een slanke, digitale en dienstverlenende overheid enerzijds en een tevreden burger en 'klant' anderzijds zijn belangrijke ambities. Daarnaast wordt ICT steeds meer ingezet voor beleid in de zorg en maatschappelijke en internationale veiligheid. Nieuwe systemen en onderlinge koppelingen daartussen moeten de veiligheid van de burger verhogen, zowel op straat als in de wereld. In alle domeinen van service, care en control geldt dat innovatief gebruikmaken van nieuwe technologische mogelijkheden een hoeksteen van modern overheidsbeleid is. Tegelijkertijd geldt dat de dynamiek van ICT ook van invloed is op de 'regels van het spel': tussen overheid en burgers, tussen overheden onderling en tussen overheid en private partijen. Informatie vloeit tussen verschillende organisaties en stroomt over publiek-private grenzen heen, zonder dat de consequenties daarvan voor burgers en overheden onderling zijn doordacht. Burgers worden steeds vaker benaderd op basis van profielen en de informatie die de overheid heeft verzameld. Daarbij staan ze veelal met lege en machteloze handen als die informatie foutief is, of foutief wordt uitgelegd. Bovendien lijkt de overheid veelal niet van plan of in staat om grenzen te stellen aan haar eigen verzamelwoede: argumenten om meer informatie te verzamelen zijn sneller gevonden dan argumenten om de nieuwsgierigheid van de overheid in te perken.

Als het gaat om nieuwe technologische mogelijkheden en in het bijzonder om de informatiestromen die daaruit voortvloeien, heeft de overheid een dubbele taak. Enerzijds heeft de overheid de dure plicht om nieuwe instrumenten, technologische innovaties en informatiestromen te verkennen om te zien of die het overheidsbeleid kunnen verbeteren. Anderzijds heeft de overheid de even dure plicht om te voorkomen dat de voorzienbare en onvoorzienbare bijeffecten van de inzet van nieuwe (informatie-)instrumenten burgers schade toebrengen (Buruma 2011). Het gebruik van ICT en de nieuwe informatiestromen die de technologie met zich meebrengt in de verschillende processen van het overheidsbeleid zijn nooit zonder gevolgen. Instrumenteel denken over technologie is op zijn best naïef en op zijn slechtst schadelijk. Nieuwe informatiestromen creëren ook nieuwe sociale en beleidsmatige werkelijkheden die gevolgen hebben voor burgers en voor overheden zelf, zo liet deel II van dit rapport zien. De overheid moet dus tussen deze twee uiteinden van het spectrum zien te laveren: ICT op innovatieve wijze gebruiken in haar beleid en beleidsuitvoering en haar burgers beschermen tegen de voorzienbare en onvoorzienbare effecten van ICT en in het bijzonder complexe informatiestromen.

Dit hoofdstuk plaatst de tendensen die in deel II zijn geanalyseerd in een nieuw kader en ontwikkelt een perspectief op een noodzakelijke paradigmawisseling. Daartoe volgt allereerst recapitulerend een schets van de belangrijkste kenmerken van de eOverheid, het voornaamste kader waarin de overheid zich momenteel verhoudt tot ICT. Vertrekkend vanuit dit kader verlegt de WRR de blik vervolgens naar een geheel ander perspectief op de informatisering van de overheid: een perspectief dat hier wordt benoemd als de iOverheid. Juist met deze andere manier van kijken komen belangrijke en prangende kwesties voor de overheid in beeld, die in het perspectief van de eOverheid en de eenzijdige focus op technologie tot op heden ten onrechte onderbelicht bleven. De focus op de informatie-Overheid volgt het pad van de informatiestromen in plaats van de individuele techniek en de losse applicaties, en toont dat deze iOverheid in empirische zin eerder 'ontstaat' dan dat deze op politiek-bestuurlijk niveau 'ontworpen' is. Deze feitelijke ontwikkeling roept vragen op over de verdere ontwikkeling van de iOverheid en de verhouding tussen burgers en overheid daarbinnen.

8.1 DE eOVERHEID

De overheid beschouwde ICT in eerste instantie vooral als een instrument om de interne organisatie en processen, met name op het terrein van uitvoering, efficiënter en effectiever te maken. Onder de term eOverheid nam ICT vervolgens een hoge vlucht en verschoof de aandacht naar 'buiten', naar beleid gericht op verbetering van dienstverlening aan burgers en bedrijven door het vergroten van effectiviteit en efficiëntie. De plannen voor en visies op de eOverheid kenmerken zich door een positieve houding ten aanzien van technologie. Dominant is de visie dat ICT een neutraal instrument is, inzetbaar om bepaalde doelen te bereiken. Daarbij is er weinig aandacht voor de context waarin ICT en eOverheid worden geïntroduceerd (Bekkers & Homburg 2009: 227). Ook is er nauwelijks tot geen aandacht voor andere (voorziene of onvoorziene) effecten die de inzet van technologie met zich mee (kan) brengen (De Mul 2003). Technologie wordt 'uitgerold', werkprocessen worden 'gestroomlijnd' en diensten 'geüpdatet'. Het technovertrouwen is groot.

Overigens is er onder de noemer van dienstverlening inmiddels wel meer en meer aandacht voor de samenhang en samenwerking tussen verschillende systemen die in de backoffice van de overheid ontstaan. Die aandacht richt zich echter hoofdzakelijk op technische aspecten als interoperabiliteit[1] en open standaarden. De inrichting en het in goede banen leiden van dit proces van vernetwerking van informatie krijgt slechts beperkt aandacht. Er is nauwelijks debat over afhankelijkheden en kwetsbaarheden die het gevolg zijn van de nieuwe samenhang, samenwerking en interoperabiliteit. Daar waar kwetsbaarheden worden erkend, worden deze soms op hun beurt getemd met een nieuwe versie van neutraliteit. Dan wordt technologie ingezet om de risico's van technologie te neutraliseren met

behulp van *privacy by design*[2] en *privacy enhancing technologies* (PETs).[3] Omdat de politieke omarming van deze nieuwe oplossingen veelal niet verdergaat dan lippendienst, worden dergelijke technologieën tot op heden nooit de oplossingen die ze wellicht zouden kunnen zijn. Een in 1999 in de Tweede Kamer aangenomen motie om in nieuwe systemen van de overheid PETs toe te passen blijft tot op heden – ondanks recent hernieuwd enthousiasme in de Kamer – grotendeels een dode letter. Bovendien blijft zo op politiek niveau de idee voortbestaan dat de inzet van technologie neutraal is. Het gegeven dat technologie veranderingen en risico's met zich meebrengt wordt meteen weer weggeredeneerd door technologie doelmatig in te zetten. De technische oriëntatie laat ook de vraag wat het betekent dat de relatie overheid-burger wordt omgevormd tot een relatie dienstverlener-consument – centraal in het eOverheidsdenken – onderbelicht. Deze nadruk op dienstverlening maakt de overheid ook kwetsbaar: ze wekt verwachtingen bij burgers die lang niet altijd waar te maken zijn, zeker in vergelijking met de op ICT gebaseerde dienstverlening door het bedrijfsleven (die overigens ook niet altijd optimaal is).

Hoewel de beleidsdocumenten een sterk geloof en vertrouwen in de mogelijkheden van ICT laten zien, brengt de eenentwintigste eeuw toch (noodgedwongen) een verbreding en nuancering van het eOverheidsdiscours. De kansen van ICT voor de overheid blijven centraal staan, maar de aandacht groeit voor barrières die de realisatie van de eOverheid in de weg staan. Zoals de ambities van een één-loket-dienst en geïntegreerde elektronische dienstverlening die tot integratie- en coördinatieproblemen leiden. In de literatuur en adviezen aan de overheid vallen steeds vaker waarschuwingen te lezen. De commissie-Postma-Wallage constateerde in 2007:

> "Een groot deel van onze gesprekpartners ziet de uitvoering van de eOverheid vooral als een 'technische' operatie, zonder duidelijke relatie met de beleidsdoelstelling. Het feit dat de politiek-bestuurlijke belangstelling nationaal en lokaal zeer beperkt is, is daar zeker debet aan. De projecten zijn te veel het domein van de technische deskundigen gebleven" (commissie-Postma-Wallage 2007: 9).

Toch blijven ook de meer recent gepresenteerde ICT-ambities van de overheid, waaronder de *ICT-Agenda 2008-2011* (ministerie van EZ 2008) spreken in termen van 'prioritaire onderwerpen' zonder daarbij tevens aandacht te hebben voor de samenhangende uitdagingen en bredere implicaties.

8.2 VAN eOVERHEID NAAR iOVERHEID

Wie verder kijkt dan de in het kader van de eOverheid ingevoerde applicaties en digitaliseringslagen ontwaart een kluwen aan informatiestromen die zich een weg

banen binnen en tussen de verschillende overheden, in de relatie burger-overheid en daarbuiten. Informatie en hoe hierop te sturen vormt echter nauwelijks een expliciet benoemd speerpunt binnen het overheidsbeleid. Stapje voor stapje, besluit na besluit, vormt er zich in de dagelijkse praktijk een informatie-Overheid zonder dat hier een overkoepelende visie of besef op het niveau van de politieke aansturing aan ten grondslag ligt. De paradox van de iOverheid bestaat erin dat de overheid een iOverheid opbouwt waar ze zelf het bestaan niet van afweet. Het ontbreken van een politiek besef 'een iOverheid te zijn' maakt dat deze in feite geen 'natuurlijke' begrenzing heeft, hetgeen wordt versterkt door de tendensen die tekenend zijn voor de ontwikkelingen zoals die zijn geschetst in deel II van dit rapport.

Effectiviteit & efficiëntie en veiligheid vormen de belangrijkste drijvende krachten achter het doorvoeren van technologische applicaties en koppelingen. Bovendien is er sprake van een groeiende verwevenheid van de beleidsdomeinen service, care en control. Ten slotte wordt binnen al die informatiestromen persoonsgerelateerde informatie steeds belangrijker. Deze tendensen brengen een aantal risico's met zich mee, waarop dit rapport de vinger wil leggen. Zo bestaat door het uitblijven van een politiek besef van de iOverheid het risico op het verlies van houvast voor de overheid. Ook kan het ontbreken van een goede organisatorische en institutionele inbedding op termijn tot externaliteiten leiden die veel aandacht, tijd en geld van de overheid zullen vergen. Ten slotte kan, wanneer kaders voor de iOverheid achterwege blijven, het vertrouwen van burgers in de overheid, en het vertrouwen binnen de overheid zelf, als betrouwbare en behoorlijke beheerder en gebruiker van informatie afnemen. Dit vertrouwen is echter noodzakelijk voor een iOverheid die innovatief wil omspringen met haar primaire processen en beleid.

8.2.1 OVER DE GRENZEN VAN DE eOVERHEID

Alhoewel het paradigma van de eOverheid als zodanig niet direct behoeft te worden losgelaten, strookt de iOverheid op belangrijke punten niet met het dominante beeld van de eOverheid. De iOverheid valt namelijk langs geheel andere lijnen te karakteriseren. In dat beeld zijn niet zozeer individuele technische faciliteiten leidend, maar informatie en informatiestromen.

Overheden hebben altijd al een natuurlijke neiging gehad tot het verzamelen van informatie om op basis daarvan in te kunnen grijpen in maatschappelijke processen. Torpey (1998) stelt dat overheden de maatschappij eerst in informationele zin omarmen om effectief te kunnen handelen. Dit impliceert dat er zo veel mogelijk informatie wordt verzameld, door middel van onder meer een uitgebreide administratieve infrastructuur, om met behulp daarvan te sturen op de volle breedte van het overheidsbeleid. Volgens onderzoek van het College Bescherming Persoonsgegevens is de gemiddelde Nederlander terug te vinden in 250 tot 500 registraties,

waarbij de ondergrens van 250 volgens de voorzitter van het CBP, Jacob Kohnstamm, behoort bij iemand die 'als een kluizenaar leeft' (Schermer & Wagemans 2009). De mogelijkheden tot het 'omarmen van de samenleving' zijn sterk gegroeid in de afgelopen jaren en zullen in de nabije toekomst alleen maar verder toenemen. De sterke groei in opslagcapaciteit en rekencapaciteit en de groeiende interoperabiliteit tussen verschillende systemen zijn de *infrastructurele* redenen waarom de feitelijke ontwikkelingen voorbij het beeld van de eOverheid gaan. Deze infrastructuur maakt een aantal inhoudelijke en organisatorische ontwikkelingen mogelijk die het karakter van de digitale overheid ook in de praktijk veranderen.

In de eerste plaats wordt technologie, zoals de voorgaande hoofdstukken duidelijk lieten zien, niet langer uitsluitend ingezet voor het verbeteren, versnellen en optimaliseren van de *dienstverlening* van de overheid, maar ook voor het verzamelen en koppelen van informatie ten behoeve van *care* en *control*. ICT speelt in toenemende mate een vitale rol in het jeugdbeleid en de gezondheidzorg (care) en is nauwelijks meer weg te denken uit het migratiebeleid en het veiligheidsbeleid, zowel als het gaat om criminaliteitsbestrijding als in het geval van antiterrorismebeleid (control). Met name op het gebied van de veiligheid lopen de informatiestromen niet alleen binnen Nederland, maar ook tussen Nederland en vele andere landen en internationale organisaties. Dankzij de infrastructuur van digitalisering en interoperabiliteit zijn de gegevens uit de in essentie losstaande kolommen van dienstverlening, zorg en controle veel gemakkelijker uitwisselbaar. Dankzij de technologie vervloeien de – toch al niet scherp afgebakende – randen tussen de verschillende kolommen.

In de tweede plaats worden netwerken, van actoren maar met name van informatie, steeds belangrijker. Binnen en buiten de overheid ontwikkelt zich een groeiende variëteit aan samenwerkingsvormen en informatiearrangementen tussen publieke en private actoren, waarbij complexe wederkerige informatie-interdependenties ontstaan. In die netwerken van informatie vermengen zich ook private en publieke informatiestromen. Overheden zijn steeds meer geïnteresseerd in de informatie die burgers en bedrijven verzamelen en maken daar ook intensief gebruik van. Waar in het geval van keteninformatisering informatie van de ene organisatie in de keten aan de andere wordt doorgegeven, geldt dat niet voor netwerken waarin informatie wordt uitgewisseld of gezamenlijk beheerd zonder dat er een vaste opvolging van actoren is. Het is opvallend dat de overheid vaak over keteninformatisering spreekt, maar veel minder over netwerkinformatisering, terwijl dat laatste de norm lijkt te worden. Het verspreiden en bewerken van informatie in netwerken geeft een dynamiek die het soms zeer lastig maakt te bepalen wie verantwoordelijkheid draagt voor (de juistheid van) bepaalde informatie over burgers. Een netwerk is ook een web waarin burgers verstrikt kunnen raken, zoals de zaak-Kowsoleea heeft laten zien.[4] Ook de Nationale Ombudsman

(2009) kon uiteindelijk geen eenduidig antwoord krijgen op de vraag hoe het complex van informatie-interactie in deze zaak van identiteitsfraude tot stand was gekomen en dus ook kon worden gecorrigeerd. Waar de eOverheid voornamelijk te maken had met het risico van grote financiële debacles bij de ontwikkeling van de systemen, liggen de risico's van de huidige ontwikkelingen veeleer in de potentiële sluipende gevolgen op informatieniveau. Die risico's betreffen zowel individuele burgers als de overheid zelf.

In de derde plaats zorgt de groei van informatiebronnen, en in het bijzonder de mogelijkheden voor koppeling en bewerking, er ook voor dat de iOverheid in toenemende mate werkt met digitale profielen en daarmee beelden van (type) burgers. Steeds vaker spelen deze een rol in het beleid en bij de beleidsuitvoering. De beelden ontstaan doordat de overheid verschillende informatiebronnen genereert en combineert door middel van het toepassen van technieken als data mining[5] op de opgeslagen informatie. Deels is dat onvermijdelijk, omdat de hoeveelheid opgeslagen informatie eenvoudigweg de menselijke maat ontstijgt en dwingt tot een elektronische verwerking daarvan en profilering daarbinnen. In de praktijk ontstaan van burgers verschillende profielen en zogenaamde *data-doubles*, dat wil zeggen een uit verschillende bronnen samengesteld profiel van een persoon dat vervolgens weer een eigen leven gaat leiden in systemen van de overheid (en/of het bedrijfsleven). Die profielen bestaan uit informatie die eerst is gedecontextualiseerd – losgemaakt uit de context waarin de informatie werd verzameld – en vervolgens wordt gehercontextualiseerd in de context van het nieuw samengesteld profiel. Die bewerking is uiteraard noch uitsluitend een technische aangelegenheid (*categories have politics*) noch zonder sociale gevolgen. Zoals al eerder werd opgemerkt (par. 4.5), hebben deze 'beelden van de toekomst' eenzelfde hinderlijk effect op de autonomie (keuzevrijheid) van burgers als 'beelden uit het verleden', die vanwege de ICT-revolutie zo lang blijven hangen. Een profiel houdt immers een prognose in van hoe (aspecten van) de identiteit van een individu er in de toekomst voor zullen staan. (Op basis van dergelijke bewerkingen wordt bovendien getracht een voorschot op de toekomst te nemen.) Profielen en informatiebewerkingen spelen in toenemende mate een rol bij opsporing (*preventive policing*) of in de jeugdzorg waar informatieverzameling en koppeling wordt gezien als een onmisbaar middel om tragedies als het Maasmeisje een volgende keer te voorkomen.

In de vierde plaats beïnvloeden de ontwikkelingen in de iSamenleving en de iOverheid elkaar. Diverse nieuwe mogelijkheden voor het verzamelen van informatie vinden hun oorsprong buiten de overheid. Nieuwe sociale media, het koop- en winkelgedrag op internet en de informatie die in de private sector wordt verzameld, genereren een potentiële goudmijn aan digitale sporen van burgers. Binnen marges en wettelijke kaders is die informatie te gebruiken voor de informatiebehoefte van de overheid. Tegelijkertijd is het ook simpelweg de aanwezigheid van

die informatie die de informatiebehoefte van de overheid voedt: er is geen natuurlijke grens die bepaalt waar informatieverzameling zou moeten stoppen en welke vermenging van publiek en privaat geoorloofd is of te ver gaat. Ook dat wordt per geval bekeken. Burgers blijken overigens een groot vertrouwen in de overheid te hebben als het gaat om het gebruik van privé-informatie door de overheid – zeker als het gaat om het verhogen van veiligheid –, maar dat is op zichzelf geen reden om geen beperking aan te brengen. Zeker niet gezien de te verwachten groei van informatie in de iSamenleving. Aan de andere kant is de overheid zelf nog weinig genegen om met burgers te interacteren of zelfs maar informatie te delen. Hoewel transparantie tot de goede voornemens van de overheid en tot de verlangens van veel burgers behoort, blijft de praktijk achter bij de goede bedoelingen. De – ook door ICT gefaciliteerde – mogelijkheden zijn aanwezig, maar het schort aan politieke wil en doorzetting. Het gevolg is dat de transparantie tussen burger en overheid eenzijdig wordt. De overvloed aan informatie in de iSamenleving in combinatie met de technologische mogelijkheden om die te ontsluiten betekent dat de overheid zal moeten nadenken over de vraag 'hoe goed zij haar eigen burgers wil kennen' en 'hoe kenbaar zij voor haar eigen burgers wil zijn'.

De feitelijke ontwikkelingen lopen dus sterk uit de pas met de traditionele focus, denkkaders en ambities van de eOverheid. De vermenging van service, care en control, de circulatie van persoonsinformatie in netwerken, de vermenging van publieke en private informatiestromen, het werken met digitale profielen waarmee een toekomstgericht proactief beleid gevoerd wordt, ontstaan als gevolg van een aaneenschakeling van besluiten over individuele applicaties, nieuwe systemen en beslissingen over koppelingen. Het de facto resultaat op een hoger niveau van abstractie is een netwerk van informatiestromen in het domein van de overheid dat ver voorbij het beleids- en denkkader van de eOverheid gaat. Critici van deze ontwikkelingen grijpen daarbij naar beelden als *Big Brother* en de *surveillance*-staat om de informatiehonger en snelle uitwisseling van informatie tussen overheidsdiensten te karakteriseren en te veroordelen. Hoewel de ontwikkelingen snel gaan, passen dergelijke beelden maar zeer ten dele bij de situatie die is ontstaan. Met name omdat deze beelden een doelbewustheid suggereren die nu juist ontbreekt: er is geen samenzwering of complot. Er is geen kwade genius die de *surveillance*-staat ontwerpt. Tegelijkertijd is dat ook bijna het probleem: de ontwikkeling van de informatieoverheid verloopt te veel de facto en is te veel een optelling van beslissingen op het niveau van individuele applicaties en beleidsbeslissingen, zonder dat er nagedacht wordt vanuit een overkoepelend besef van het grotere geheel. Dat besef mist en kan zeker niet gevonden worden in de taal van de eOverheid. Sterker nog, het is juist dit discours van de eOverheid dat de ontwikkelingen depolitiseert, instrumentaliseert en neutraliseert, terwijl de ontwikkelingen om het tegenovergestelde daarvan vragen.

Figuur 8.1 De iOverheid verbeeld



8.2.2 iOVERHEID

Om de in dit rapport geschetste ontwikkelingen te analyseren en handvatten te bieden voor nieuw beleid is de term 'iOverheid' de aangewezen term. De iOverheid, oftewel de informatie-Overheid, is in de termen van Mayer-Schönberger & Lazer (2007: 5) een "conceptual lens that offers a complementary perspective to understand the changing nature of government and its relationship to the citizenry". De term iOverheid duidt dus niet alleen op het *feitelijke ontstaan* van een andere overheid als gevolg van de geschetste ontwikkelingen, maar staat tegelijk ook voor een andere manier van kijken naar die overheid. Bij de iOverheid ligt de nadruk op informatiestromen en pas in het verlengde daarvan op de technologie die deze informatiestromen mogelijk maakt. Dat is van groot belang, omdat het politieke en maatschappelijke debat in Nederland altijd begint, en vaak ook eindigt, met de technologie of de specifieke technologische applicatie zelf. De lens van de iOverheid maakt door de nadruk op informatiestromen ook duidelijk dat de ontwikkelingen die in dit rapport zijn besproken in de praktijk veel meer samenhang hebben dan de discussie over individuele technieken en applicaties doet vermoeden. En als laatste brengt de lens van de iOverheid aan het licht dat de Nederlandse overheid, ondanks enkele zeer bescheiden aanzetten, geen noemenswaardig besef heeft van het bestaan en de consequenties van deze iOverheid en dus ook niet vanuit dat besef de ontwikkelingen binnen en buiten de overheid kan beoordelen en sturen. Dat besef is nodig omdat de de facto ontwikkeling van de iOverheid twee kenmerken heeft die bij elkaar opgeteld ongewenst zijn. De ontwikkeling van de iOverheid is een paradox in termen van politieke aansturing en deze paradox maakt het mogelijk dat de ontwikkeling van de iOverheid geen natuurlijke begrenzing heeft.

8.3 DE PARADOX VAN DE iOVERHEID

De ontwikkeling van de iOverheid is een politieke paradox: de iOverheid is niet gelegitimeerd vanuit een expliciete politieke keuze, maar is het resultaat van de vele politieke en beleidsmatige keuzes op het niveau van individuele technische applicaties en koppelingen. Tegelijkertijd zijn die individuele keuzes geen toevalligheden, maar welbewuste politieke en beleidsmatige beslissingen.

8.3.1 POLITIEKE KEUZES OP HET NIVEAU VAN APPLICATIES CREËREN EEN iOVERHEID

De oorsprong van de iOverheid ligt bij de actoren die de nieuwe mogelijkheden die ICT te bieden heeft voor het realiseren van hun beleidsopdracht en ambities, signaleren, ter hand nemen, ontwikkelen en ermee aan de slag gaan. Vaak wordt er een scala aan motieven gepresenteerd om de inzet van ICT voor een bepaald beleidsdoel aannemelijk te maken, waarbij een hoofdrol is weggelegd voor de

stuwende beginselen van veiligheid en effectiviteit & efficiëntie. Technovertrouwen en de wens om systemen politiek te 'verkopen' spelen in die argumentaties ook een rol. Het empirische materiaal laat zien dat dit resulteert in een waaier van initiatieven die stuk voor stuk beleidsmatig en politiek aangestuurd en beoordeeld worden. Het betreft hier echter iedere keer geïsoleerde beslissingen gericht op afzonderlijke applicaties, ICT-programma's en beleidsdoelstellingen. De aandacht gaat zelden tot nooit uit naar de via de applicaties gegenereerde informatiestromen en hoe deze stromen verder vorm en inhoud krijgen in het grotere geheel van informatieprocessen binnen de overheid. Vaak worden beslissingen over nieuwe koppelingen of toegang tot informatiestromen voor weer andere organisaties ook op een later tijdstip, als weer een nieuwe individuele beslissing, genomen. *Function creep* is een proces dat zich vaak over jaren uitstrekt, maar dat wel een zekere voorspelbaarheid in zich heeft. De omvang en effecten van het koppelen van informatie lijken zich vaak volledig te onttrekken aan het zicht van niet alleen het bredere publiek, maar ook van de overheid zelf. Er is dikwijls nog wel oog voor de afgebakende informatiestromen binnen een beleidsterrein, de informatiestroom die voortkomt uit een specifieke applicatie, of een individuele koppeling. Maar men kijkt niet naar de betekenis van informatiestromen wanneer die verder worden gekoppeld, door verschillende beleidsdomeinen stromen en opgaan in bredere informatienetwerken.

8.3.2 ZONDER POLITIEK BESEF VAN EN KEUZE VÓÓR DE iOVERHEID

Er is niet alleen onvoldoende oog voor en besef van de ontwikkelingen op hoog politiek-bestuurlijk niveau, maar mede daardoor ontbreekt het ook aan een kader om die ontwikkelingen in goede banen te leiden. De iOverheid is eerder ontstaan dan dat zij ontworpen is. Juist omdat er geen ontwerp aan ten grondslag ligt, is een complex en gedifferentieerd stelsel van formele en informele beleids-, ontwikkel- en implementatietrajecten ontstaan die per initiatief en beleidsonderwerp verschillen. Per departement, per maatregel en per systeem ontstaat een vervlechting van informatiestromen waarbij de grenzen niet van nature zijn gegeven. In feite is er nog geen begin van een gedachte wat de ontwikkeling van de iOverheid betekent voor zowel het overheidsfunctioneren, de inrichting van processen en de manier waarop overheid en burger zich tot elkaar verhouden en naar elkaar kijken. De feitelijke ontwikkeling van de iOverheid loopt eigenlijk mijlenver voor op het politiek-bestuurlijke kader dat daarbij hoort.

8.4 DE ONBEGRENSDE iOVERHEID

De opeenstapeling van ad-hocbesluiten enerzijds en het ontbreken van 'een besef van' anderzijds maken dat de iOverheid zich als het ware onbegrensd en daarmee 'grenzeloos' ontwikkelt. De grenzen van de verknoping en uitwaaiering van individuele applicaties zijn niet gegeven, omdat niemand zich hoeder voelt van

het geheel. Specialismen en kolommen, zowel in politiek als bestuur, en de (financiële) belangen die daarbij horen, staan een bredere oriëntatie in de weg. Het legt de vraag op tafel wie de bredere ontwikkeling op het niveau van de iOverheid beoordeelt en – waar nodig – inperkt. Voor alle volgende observaties geldt dan ook: tot hoe ver kunnen de ontwikkelingen gaan?

Een eerste observatie is dat op het niveau van individuele applicaties en koppelingen stuwende beginselen als effectiviteit & efficiëntie en veiligheid keer op keer de belangrijke krachten zijn voor het doorvoeren van technologische applicaties en koppelingen. Zo is, zeker na 9/11, in het kader van veiligheid en controle menig database opgetuigd om een herhaling te voorkomen. De dynamiek binnen het EU-beleidsterrein van Justitie en Binnenlandse Zaken is een mooi voorbeeld waarin gegevensbescherming keer op keer heeft moeten wijken voor veiligheid. Dat gebeurde overigens met een minimum aan parlementaire controle. Maar ook het technovertrouwen en daarmee de populariteit van fenomenen als voorspellend rechercheren (*predictive policing*) en proactief sturen op toekomstig gedrag van burgers staat de laatste jaren sterk op de voorgrond. Hierdoor komen begrippen als 'onschuldig tot schuld is bewezen' en 'vergeven is vergeten' in het strafrecht onder druk te staan. Door de nadruk op effectiviteit & efficiëntie en veiligheid delven verankerende beginselen als keuzevrijheid en privacy vaak het onderspit in de afweging. Op het niveau van individuele applicaties en koppelingen is altijd een goede (politieke) reden te vinden waarom veiligheid bij deze specifieke applicatie het zwaarst moet wegen – nood breekt immers wet –, maar de optelsom van al die individuele afwegingen wordt nooit meegenomen als er geen besef is van het resultaat op geaggregeerd niveau. Daarom toont het gebrek aan begrenzing zich het sterkst in de vertaling van individuele applicaties naar het niveau van de samenhang van de iOverheid. Weliswaar vindt bij elke nieuw in te voeren applicatie of initiatief een politiek-bestuurlijke afweging plaats tussen de met het initiatief gediende beginselen, zoals veiligheid, privacy of keuzevrijheid, maar deze afweging adresseert niet de weging van deze beginselen op niveau van de geaggregeerde informatiestromen, op het niveau van de iOverheid als geheel. Dit terwijl de applicatie uiteindelijk wel onderdeel wordt van die iOverheid in ontwikkeling.

Bovendien toont het gebrek aan begrenzing zich in de groeiende verwevenheid van de beleidsdomeinen dienstverlening, zorg en controle, waarbij de informatisering met name op het gebied van care en control snel is toegenomen. De nadruk op effectiviteit & efficiëntie en veiligheid maakt het aantrekkelijk – en politiek te verantwoorden – dat barrières tussen verschillende informatiestromen worden geslecht om de veiligheid te vergroten of om controle of dienstverlening omvattender en efficiënter te maken. Zoals de hoofdstukken in deel II aan de hand van diverse illustraties duidelijk maken, worden binnen de jeugdzorg de domeinen zorg en controle (sociale veiligheid) bij elkaar gebracht, interfereren controle en dienstverlening bij initiatieven van de politie op het internet en speelt de ontwik-

keling van het eRijbewijs in op nieuwe ambities rondom zowel dienstverlening als controle. Gefaciliteerd door unieke identificatiesleutels (waaronder het BSN en biometrie) wordt het mogelijk zeer uiteenlopende inhoudelijke informatie vast te klinken aan een persoon en die gegevens vervolgens over de grenzen van de voorheen geïsoleerde beleidscontext en het gesloten institutionele circuit heen uit te wisselen. Deze gegevens kunnen vervolgens in een nieuwe samenhang en context gebruikt worden. Onder invloed van deze ontwikkelingen nemen organisaties ook hun eigen rol en ambities onder de loep. Her en der betekent dit dat werkprocessen en werkterreinen worden aangepast en verruimd door ook voor beleidsterreinen waar men voorheen niet op was georiënteerd, nieuwe producten en diensten te ontwikkelen. Kijkend vanuit het perspectief van informatiestromen en gegevensbenutting lijken de drie beleidsdomeinen zorg, controle en dienstverlening in toenemende mate een geïntegreerd onderdeel van het bestuur te worden. Terwijl ze wat betreft de bestuurlijke infrastructuur, verantwoordelijkheidsmechanismen, juridische spelregels en andere kaders verre van vergelijkbaar en zomaar te integreren zijn. Het resultaat is een spanningsveld rondom taken, bevoegdheden en verantwoordelijkheden. In het bijzonder omdat door de verwevenheid ineens ook actoren uit ‘vreemde’ hoek op het toneel van zorg, controle en dienstverlening verschijnen, waaronder diverse partijen uit de private sector.

8.5 GEVOLGEN VAN EEN ONBEGRENSDE iOVERHEID

De ‘onbegrensde’ iOverheid brengt risico’s en knelpunten met zich mee, niet alleen direct, maar ook in de zin dat kansen om de potentie van de iOverheid te benutten, blijven liggen, dan wel onvoldoende worden benut. Bij de verdere ontwikkeling van de iOverheid moet daarom met een aantal risico’s terdege rekening worden gehouden.

8.5.1 VERTEKEND BEELD

Een eerste risico dat de overheid loopt, is dat het houvast dat ze in een afgezonderd beleidsdomein denkt te vinden in informatietechnologie, over het geheel beschouwd – wanneer de technisch verknoopte informatiesystemen in samenhang worden bezien – kan verkeren in het tegendeel. De geschetste systeem-per-systeembenadering maakt dat in de beoordeling de individuele toepassing in de geïsoleerde beleidscontext centraal staat, in plaats van in de context van reeds bestaande technieken, applicaties en informatiesystemen waarin die nieuwe toepassing komt te functioneren. Daarmee ontbreekt een scherp beeld van en kritische reflectie op de bredere implicaties van een concreet initiatief. Uiteindelijk ontstaat zo ook een vertekend beeld. De achterliggende en bredere belangen, problemen en afbreukrisico’s die juist bij het vervlechten van initiatieven naar voren treden, worden onvoldoende gezien, erkend en in de beoordeling betrokken. Deze blinde vlek op het niveau van de samenhang van informatiestromen

maakt dat de overheid dus ook voor verrassingen komt te staan. Identiteitsfraude is hiervan een voorbeeld. Nu nog lijkt het een relatief klein fenomeen, maar de inventarisatie van de achterliggende problemen staat nog in de kinderschoenen. De vermenging van informatie, alsmede de bewerking en de decontextualisering daarvan hebben ook gevolgen voor de kwaliteit en betrouwbaarheid voor informatie. Hoewel de bedoeling is om controle te vergroten, kan gebrekkige kwaliteit van informatie de blik van de overheid vertroebelen, het onderling vertrouwen tussen overheidsinstanties onder druk zetten en daarmee juist de controle doen afnemen. Identiteitsverwarring, verkeerde en verouderde registraties met reële gevolgen, burgers die vastlopen in digitale overheidsnetwerken komen meer en meer voor. Het risico tekent zich af dat politiek en beleid het regisserend vermogen kwijtraken, en ervoor zullen moeten waken dat de negatieve effecten van een ondoordachte iOverheid zwaarder gaan wegen dan de vruchten van de informatisering.

8.5.2 ONTBREKEN VAN NOODZAKELIJKE ORGANISATORISCHE EN INSTITUTIONELE INBEDDING

Het tweede risico hangt samen met de observatie dat in het huidige discours wordt geredeneerd vanuit technologische systemen in plaats van organisatorische processen. De focus ligt op het product en niet op het proces. Het politieke en bestuurlijke debat richt zich op een applicatie, of soms zelfs op een deelaspect van een applicatie zoals in het geval van de veiligheid van de OV-chipkaart. Daardoor valt het bredere proces en het informatienetwerk waar een applicatie deel van uit gaat maken – meteen bij de start en door latere besluiten voor koppelingen – goeddeels buiten de discussie. Het gevolg is dat het benutten van de technologische mogelijkheden in het debat veelal centraal staat, terwijl de organisatorische en institutionele inbedding buiten beeld blijft of naar de achtergrond verdwijnt. Toch is juist deze inbedding van doorslaggevend belang voor het borgen van de publieke kwaliteitseisen – met name de procesmatige beginselen van accountability en transparantie – als het systeem eenmaal operationeel is. Als de iOverheid zodanig dominant wordt dat organisaties op het niveau van informatiestromen verknoopt raken, zal het ontbreken van de daarmee samenhangende ‘verknoping’ op organisatorisch en institutioneel niveau in toenemende mate problematisch worden. Vragen van verantwoordelijkheid en transparantie moeten juridisch en organisatorisch worden doorvertaald naar de schaal van de iOverheid om te voorkomen dat ze wegglippen tussen de kieren van de huidige organisatiestructuur. Ook het toezicht is grotendeels nog toegesneden op de eOverheid en beperkt zich, of is wettelijk beperkt tot, de kokers van de individuele beleidsterreinen. Het bredere perspectief van de iOverheid sluit slecht aan bij de manier waarop ministeries, Kamercommissies, toezichthouders, rechtsbeschermings- en klachtenprocedures zijn ingericht. Voor burgers is het echter van vitaal belang om te weten waar verantwoordelijkheid is belegd en voor de overheid is dat van vitaal belang om de

kwaliteit van informatie op peil te houden en het vertrouwen van burgers in de iOverheid te waarborgen voor de langere termijn.

8.5.3 VERTROUWEN EN INNOVATIE

Het derde risico dat verband houdt met het gebrek aan begrenzing is dat het vertrouwen van burgers in de overheid als betrouwbare en behoorlijke beheerder en gebruiker van informatie afbrokkelt. Zonder een fundamentele reflectie op de kenmerken, randvoorwaarden, maar ook nieuwe risico's maakt de iOverheid zich kwetsbaar (vanuit het geloof in een perfect werkende technologie) en bovendien afhankelijk van digitale systemen en daarin opgeslagen informatie (systeem- en informatiefalen). Zonder deze reflectie komen zaken als goed opdrachtgeverschap, transparantie en accountability in het geding, terwijl dit juist noodzakelijke eigenschappen zijn van een overheid die vertrouwen inboezemt. De overheid moet kunnen waarborgen dat informatiestromen binnen haar eigen systemen, maar ook tot op een bepaalde hoogte daarbuiten, niet zodanig uit de rails lopen dat burgers daardoor schade wordt berokkend.

Alhoewel het te vroeg is hier eenduidige conclusies aan te verbinden, tonen zich eerste kleine scheurtjes in het vertrouwen van burgers. Illustratief is het flinke aantal bezwaren tegen het EPD, de meer extreme actie van de burgerbeweging Het Nieuwe Rijk waarbij met een gepersifleerde brochure het overheidsbeleid wordt gehekeld door te suggereren dat het BSN op de arm kan worden getatoeëerd, en de procedures die organisaties als Vrijbit en Privacy First hebben aangespannen over de centrale opslag van vingerafdrukken van alle Nederlanders met een (nieuw) paspoort. In Nederland lijken de zorgen onder de bevolking nog relatief beperkt in vergelijking met ons omringende landen zoals Duitsland waar een sterke burgerbeweging op deze thematiek actief is. Grote en breed in de media uitgemeten zaken als de T-Mobile-affaire in Duitsland en de grootschalige *data breaches* in Engeland kunnen het vertrouwen van burgers sterk op de proef stellen.[6] Ook in Nederland kan het vertrouwen kwetsbaar blijken. In ieder geval, zo blijkt uit de in opdracht van ECP-EPN en de WRR uitgevoerde enquête, hangen opvattingen over het gebruik van persoonsgegevens nauw samen met de specifieke context waarin en het oogmerk waarvoor dat gebruik plaatsvindt (Attema & De Nood 2010: 2). Het is ook deze constatering die erop duidt dat de overheid het belang van begrenzing dient te onderkennen.

Afbreukrisico's rondom vertrouwen spelen niet alleen in de relatie overheid-burger, maar ook binnen de overheid zelf, in het bijzonder tussen beleid en uitvoering. Zowel binnen de departementen als op uitvoeringsniveau wordt een sterke behoefte geuit aan duidelijke bakens, mede om een werkbare aansturing op uitvoeringsniveau te verzekeren. Juist vanwege het ontbreken van een politiek-bestuurlijk besef van de iOverheid en kaders voor de verdere ontwikkeling daarvan lijkt de afstand tussen beleid en uitvoering te groeien. Het adresseren van deze

afstand is daarom niet alleen van groot belang voor de slagkracht van de overheid (en daarmee ook de iOverheid), maar ook voor het vertrouwen van verschillende partijen binnen de overheid zelf.Bovendien heeft de overheid ook vertrouwen nodig om voldoende te kunnen innoveren. Het vermogen om met behulp van technologie en informatie te innoveren, is immers een voorwaarde om de kansen die een doordachte iOverheid biedt te kunnen benutten. Vertrouwen is nodig om met de onzekerheid die innovatie kenmerkt om te gaan.

"Innovatie is per definitie onvoorspelbaar en beleid met betrekking tot innovatie moet hier dan ook rekening mee houden. Deze inherente onzekerheid betekent dat effectief innovatiebeleid onmogelijk vooraf de gewenste doelen en middelen kan vastleggen. Ook betekent dit dat rekening gehouden moet worden met vele mislukkingen, die noodzakelijk zijn om tot waardevolle vernieuwingen te komen" (WRR 2008a: 9-10).

Om de onzekerheid die met innovatie gepaard gaat als ook de mislukkingen die het inherent met zich meebrengt te kunnen dragen is vertrouwen nodig. Burgers moeten ervan opaan kunnen dat verantwoordelijkheden voor mogelijk falen rechtvaardig belegd zijn en geen onnodige risico's worden genomen. De onzekerheid en mislukkingen die inherent zijn aan innovatie zijn alleen maar aanvaardbaar wanneer er een duidelijk kader is waarbinnen innovatieve processen plaatsvinden.

8.6 EEN VAN ZICHZELF BEWUSTE iOVERHEID

De kernanalyse van dit rapport is dat met de inzet van ICT en in het bijzonder het benutten van informatie(stromen) zowel (beleids)processen als sociale werkelijkheden sterk veranderen en dat daarmee de facto een andere overheid in ontwikkeling is. Dit is een overheid die dit rapport duidt als de iOverheid. De iOverheid, zo betoogt dit rapport, kenmerkt zich door een focus op informatiestromen en processen die daarmee verband houden. Technologie is daarbij niet leidend, maar veeleer faciliterend. Het ontstaan van deze iOverheid blijkt, zo laat de analyse zien, een incrementeel proces van *feitelijke* opeenstapelingen van initiatieven, die door de betrokken actoren onvoldoende onderkend en bevraagd worden. Alhoewel de iOverheid feitelijk nog sterk in opbouw en ontwikkeling is, en begripsmatig nog nauwelijks op de radar is verschenen, heeft ze wel degelijk al reële gevolgen, zoals de empirische analyse laat zien. Door dit gebrekkige 'bewustzijn' worden de karakteristieken van de iOverheid nauwelijks in de beleidsontwikkeling betrokken en ontbreekt het aan een goed politiek-bestuurlijk besef van *wat* zich ontwikkelt, laat staan van een besef *hoe* die ontwikkeling in goede banen geleid kan worden. Dit noopt tot een andere oriëntatie van beleid en politiek. Alles wijst erop dat de iOverheid 'van nature' verder zal gaan op de ingeslagen weg: dat zij meer en meer gestalte krijgt via de continue uitbouw op het niveau van applicaties en informatiestromen.

Om het momenteel duidelijk onderontwikkelde zicht op zowel dit proces als de gevolgen daarvan te verbeteren, zal de focus verlegd moeten worden. Niet langer zal deze primair gericht moeten zijn op het product, de applicatie, maar op het daaruit resulterende proces, de informatiestromen. Het beleid, maar ook de nog te bespreken procedures en waarborgen, zullen zich rekenschap dienen te geven van het mozaïek van informatiestromen en de beleidsmatige en sociale gevolgen daarvan. Op het meeste basale niveau betekent dit het volgende.

De overheid dient in alle geledingen te beseffen dat zij onder invloed van ICT is veranderd van een eOverheid in een iOverheid. Een iOverheid stelt andere eisen aan de inzet van beleid, het functioneren van overheidsinstellingen en de waarborgen voor burgers.

Het perspectief van de iOverheid brengt, zoals betoogd, een aantal lacunes aan het licht in de manier waarop de eOverheid momenteel te werk gaat. Met name is het geheel, het verdichtende web van dwarsverbanden, onvoldoende scherp in beeld en onvoldoende beleidsmatig en institutioneel omlijst. In het volgende hoofdstuk wordt daarom geschetst hoe er vanuit 'het besef van de iOverheid' kan worden gedacht over manieren waarop een meer bewuste en evenwichtige omgang met deze lacunes mogelijk is. Het betreft daarbij niet alleen normatieve en procedurele manieren om het besef handen en voeten te geven, maar ook richtingen voor de noodzakelijke institutionele verankering.

NOTEN

1 Interoperabiliteit betekent dat systemen (of applicaties) in staat zijn tot onderlinge uitwisseling of/en communicatie. Om interoperabiliteit te bereiken zijn standaarden, protocollen en procedures belangrijk.

2 Privacy Enhancing Technologies (PET) is de verzamelnaam voor verschillende technieken in informatiesystemen om de bescherming van persoonsgegevens te ondersteunen.

3 Privacy by Design gaat uit van het principe dat er in een vroeg stadium nagedacht wordt over het juiste gebruik van persoonsgegevens binnen een organisatie, de noodzaak van het gebruik van deze gegevens en de bescherming ervan. Gegevensbescherming inclusief PET dient van meet af aan een onderdeel te zijn van het ontwerp van de architectuur van het informatiesysteem.

4 Door fraude met zijn identiteit stond Ron Kowsoleea dertien jaar onterecht geregistreerd als harddrugscrimineel in informatiesystemen van de overheid. Een drugsverslaafde bleek zich voor hem uit te geven. Door de fraude stond hij geregistreerd als ongewenste vreemdeling, had onterecht een strafblad, ontving onterecht bekeuringen, had problemen met reizen via Schiphol en is de FIOD zijn huis binnengevallen in het bijzijn van zijn twee kinderen. Onderzoek van de Nationale Ombudsman laat zien hoeveel moeite het politie, justitie en de Koninklijke Marechaussee kostte de onjuiste registraties te verwijderen (Nationale Ombudsman, persbericht 23 oktober 2008).

5 Data mining (ook wel *predictive analytics* of *knowledge discovery from databases*) kan bijna letterlijk worden vertaald als het opgraven van informatie uit databases. Zonder data mining beperkt een data-analyse zich tot een klein aantal aspecten waarvan men vermoedt dat ze een rol spelen. Met data mining wordt de scope van de analyse enorm vergroot. Door het toepassen van kunstmatige intelligentie, statistische technieken en visuele rapportagemethoden worden alle verborgen patronen en verbanden gevonden. Zo wordt het mogelijk om grote gegevensverzamelingen te analyseren en complexe verbanden te ontdekken.

6 In Duitsland zijn in 2006 meer dan zeventien miljoen klantgegevens van T-Mobile gestolen. Het ging om (geheime) nummers van mobiele telefoons, adressen, geboortedata en e-mailadressen die via internet aan criminelen aangeboden werden. Engeland kende de afgelopen jaren een serie van *data breaches* (dataverlies: het onbedoeld vrijgeven van beveiligde informatie in een niet-gecontroleerde context), zoals het verlies van twee dvd's met gegevens van 25 miljoen kinderbijslaggegevens (november 2007); een gestolen laptop met persoonsinformatie van 600.000 marineofficieren (januari 2008); zes gestolen laptops met patiëntengegevens van 20.000 patiënten (juni 2008) (www.bbc.co.uk, geraadpleegd op 22 januari 2009). Zie voor Nederlandse voorbeelden het overzicht bijgehouden door Bits of Freedom (www.bof.nl).

9 aanbevelingen: werken aan de iOverheid

De overheid dient te beseffen dat ze een iOverheid is. Dat besef is van vitaal belang om enerzijds de uitdagingen van de almaar verdergaande digitalisering het hoofd te bieden en anderzijds innovatie met behulp van digitalisering te kunnen benutten. Redeneren vanuit het besef 'een iOverheid te zijn' betekent dat de overheid verder kijkt dan naar de techniek en individuele applicaties, maar de blik verlegt naar het perspectief van de iOverheid. Vanuit dat perspectief dient de aandacht uit te gaan naar de informatiestromen die het resultaat zijn van de vele applicaties en koppelingen daartussen. Bovenal moet de aandacht zich richten op de maatschappelijke en beleidsmatige gevolgen van continue uitbouw en dynamiek van de iOverheid.

Het is verleidelijk om voor de noodzakelijke transformatie en de daarmee samenhangende maatregelen een departement, organisatie of ambt aan te wijzen: één centraal punt dat vanuit een totaaloverzicht op de iOverheid de verantwoordelijkheid daarvoor draagt. Dat is echter een grotendeels onbegaanbare weg, gezien de omvang, complexiteit en gedetailleerdheid van de implicaties van ICT voor de relatie burger-overheid. Dit rapport kan geen alomvattende strategie of een blauwdruk voor een evenwichtige ontwikkeling van de iOverheid leveren en verwacht ook niet dat 'de' overheid dat kan. Het besef van de iOverheid en de consequenties daarvan zullen moeten inzinken in de vele lagen en instituties van de overheid: departementen, agentschappen, gemeenten, politie, toezichthouders, burgers en, *last but not least*, politici. De iOverheid is de facto ontstaan op vele plekken binnen de overheid en het besef van de consequenties daarvan zal dezelfde weg moeten volgen. Dat gezegd zijnde geldt natuurlijk altijd dat sommigen meer gelijk zijn dan anderen. In dit laatste hoofdstuk wordt aan enkele organisaties een grote verantwoordelijkheid toebedeeld om dit besef uit te dragen en de consequenties van deze ontwikkelingen in goede banen te leiden. Deze 'taken' moeten worden gezien als de organisatorische uitwerking van een agenda van transformatie voor de Nederlandse overheid. De transformatie van een eOverheid naar een iOverheid is een paradigmawisseling die zich de facto al heeft ontvouwd, maar nu ook hoognodig ingebed moet worden in het denken en de instituties van de Nederlandse overheid. Daarbij geldt dat de transformatieve agenda veel belangrijker is dan de concrete suggesties voor de institutionele inbedding daarvan. Er zijn meerdere wegen die naar Rome leiden, maar de overheid kan het zich niet veroorloven om niet in Rome aan te komen.

Vanuit deze observatie wordt in de eerste drie paragrafen van dit hoofdstuk een aantal normatieve en procedurele aanbevelingen uitgewerkt. Paragraaf 9.1 formuleert daartoe allereerst aanbevelingen op het niveau van de driedeling in stuwende, verankerende en procedurele beginselen die eerder in dit rapport werden

gepresenteerd en in de empirische analyse een belangrijke rol speelden. Paragraaf 9.2 onderscheidt vervolgens op basis van deze analyse een drietal karakteristieken van informatie die als 'waarschuwingsvlaggen' hebben te gelden voor een bewuste iOverheid. Het gaat daarbij niet om typen informatie, maar om *kenmerken* van informatie die om speciale waarborgen vragen, zowel voor de overheid zelf als in de relatie overheid-burger. Aan de hand van deze waarborgen worden in paragraaf 9.2 twee aanbevelingen geformuleerd, die daarmee ook de opmaat vormen tot de noodzakelijke reflectie, aangekaart in subparagraaf 9.2.3, over de begrenzing van de iOverheid. Ten slotte presenteert paragraaf 9.3 de ingrediënten voor de institutionele inrichting om het besef 'een iOverheid te zijn' te verankeren.

9.1 EXPLICIETE AFWEGING VAN STUWENDE, VERANKERENDE EN PROCEDURELE BEGINSELEN

De dynamiek tussen de stuwende beginselen – zoals effectiviteit & efficiëntie en veiligheid – en de verankerende beginselen – zoals privacy en keuzevrijheid – is, zo laat de empirie zien, sterk sturend voor de ontwikkeling van de iOverheid. Ook de invulling van procedurele noties zoals transparantie en accountability laat zien wat de moeilijkheden, mogelijkheden en (gemiste) kansen zijn om de ontwikkeling van de iOverheid normatief-institutioneel in te bedden. Op de persoon af gevraagd zal nagenoeg elke bestuurder, politicus en ambtenaar het belang van *al* deze beginselen onderschrijven. Ze appelleren immers allemaal aan gezond verstand, verantwoordelijkheid, grondwettelijke waarden en zorgvuldigheid. Niemand is faliekant tegen veiligheid of tegen privacy, om die twee begrippen die het vaakst tegen elkaar uitgespeeld worden maar als voorbeeld te nemen. Wederom op de persoon af gevraagd zal iedereen zeggen dat deze beginselen in een zorgvuldig proces onderling tegen elkaar afgewogen moeten worden. Besluitvorming moet immers altijd gebalanceerd zijn. In theorie althans kan men het in de regel wel met elkaar eens worden. De praktijk, zo blijkt uit de analyse in deel II van dit rapport, is echter vaak een heel andere. ICT is – het is eerder gezegd – vaak veel meer een politieke keuze dan een puur instrumentele oplossing voor een probleem. En politiek is nu eenmaal strijd. In de dagelijkse werkelijkheid van de iOverheid in wording is de afweging van de verschillende beginselen in de regel een minder evenwichtige en openbare aangelegenheid dan de theorie doet vermoeden. Dat heeft een aantal redenen: a) de beginselen worden zelden expliciet gemaakt en openlijk bediscussieerd, b) de beginselen zijn ongelijksoortig en daarom moeilijk te duiden en tegen elkaar af te wegen en c) er valt politiek en bestuurlijk wat te winnen bij een onevenwichtige voorstelling van zaken. Deze redenen worden hieronder uitgewerkt en in het licht geplaatst van een tweetal aanbevelingen om de afwegingen en het debat over de iOverheid op het niveau van de beginselen meer open, expliciet en realistisch vorm te geven.

De drie in dit rapport gehanteerde clusters van beginselen – stuwend, verankerend en procesmatig – moeten op alle niveaus waar beslissingen worden genomen met elkaar in balans worden gebracht. Dit is geen geringe opgave, aangezien een kwantitatief getint concept als efficiëntie enerzijds, en een meer normatief concept als keuzevrijheid of een procesmatig concept als accountability anderzijds, duidelijk in verschillende registers van analyse thuishoren. Stuwende beginselen zoals efficiëntie en veiligheid hebben bovendien, zo laat de empirie zien, weinig steun in de rug nodig om voor het voetlicht te treden.

Voor de verankerende beginselen ligt dat vaak anders. Zij zijn gegrond in de vrijheid en autonomie van burgers en uitgewerkt in de beginselen privacy en keuzevrijheid. Ondanks de absolute en grondrechtelijke klank van het begrip vrijheid, blijken deze noties in de praktijk van alledag veel plooibaarder dan de argumenten die aan de andere kant van de balans, in het domein van efficiëntie en veiligheid, worden neergelegd. Het argument voor verankering ligt veelal in de potentiële schending van individuele belangen die in een afweging soms eenvoudig het onderspit delven tegen de gepercipieerde belangen van het collectief. De privacy van individuen weegt daarmee vaak niet op tegen de veiligheid van het collectief. De spil van de toezichthoudende en rechterlijke toetsing wordt vrijwel altijd gevormd door de vraag of de inbreuk op een grondrecht evenredig is. Er is eigenlijk geen gemeenschappelijke eenheid of valuta die een quasimathematische afweging tussen deze ongelijksoortige categorieën van beginselen (stuwend enerzijds, verankerend anderzijds) mogelijk maakt. Wanneer toch wordt gepoogd de afweging in één bepaald keurslijf te dwingen – bijvoorbeeld in een kosten-baten-analyse – dan bestaat het risico dat de overwegingen (en de taal) van effectiviteit & efficiëntie de overhand krijgen.

Voor het vinden van een juiste balans tussen de stuwende en de verankerende beginselen van de iOverheid komt in de praktijk veel aan op de intermediaire procesmatige beginselen accountability en transparantie. Zonder een stevige invulling van deze noties dreigt elke afweging in de lucht te blijven hangen. De beginselen van accountability en transparantie moeten de toetsbaarheid van het proces van ontwikkeling van de iOverheid waarborgen. Ze eisen tezamen dat de vaak impliciete afwegingen die de overheid maakt, inzichtelijk, navolgbaar, bediscussieerbaar en aanvechtbaar worden gemaakt. Eigenlijk is de enige in deze context geloofwaardige manier om de verschillende beginselen tegen elkaar af te wegen een argumentatieve manier. Om die argumentaties het vrije spel te geven is het nodig dat de overheid haar eigen afwegingen zo expliciet mogelijk wereldkundig maakt. Een van de belangrijkste agendapunten voor de iOverheid is de eis dat de afwegingen op beginselniveau (die onvermijdelijk moeten plaatsvinden) expliciet worden gemaakt. Deze afweging moet op alle niveaus geëxpliciteerd worden: van de voorbereiding en introductie van een concrete toepassing tot aan de omvattende vertakking van processen en informatiestromen waaruit de iOverheid is

opgebouwd. Dat geldt niet alleen voor het nationale niveau, maar ook voor de afwegingen die op het internationale, en met name op het Europese niveau worden gemaakt. Dat verlangt dat de Nederlandse regering in een tijdig stadium expliciteert met welke afweging zij aan de Europese vergadertafel plaatsneemt en met welk resultaat, in termen van afweging, zij wenst thuis te komen. Dit leidt tot de eerste aanbeveling op het niveau van de beginselen.

Een evenwichtige ontwikkeling van de iOverheid vereist een doordachte afweging tussen de stuwende, verankerende en procesmatige beginselen die geëxpliciteerd, toetsbaar en publiekelijk te verantwoorden is.

De noodzaak van een omvattende en publiek te verantwoorden afweging is groot, omdat een eenzijdige benadering van de beginselen en daarmee de iOverheid op den duur ongewenste gevolgen heeft. Voor alle beginselen geldt dat het eenzijdig najagen van een enkel beginsel (veiligheid/privacy/transparantie boven alles!) er uiteindelijk voor zorgt dat de iOverheid applicatie voor applicatie en koppeling na koppeling in een extreme, onwerkbare en kwetsbare vorm uitmondt. Het is daarom belangrijk om een open oog te houden voor signalen en indicaties dat een of meerdere van deze beginselen de overige gaan verstikken. Juist voor beginselen geldt dat de maatschappij er te weinig maar evengoed te veel van kan hebben. Dat potentiële gevaar van dominantie bestaat voor *alle* beginselen, zeker wanneer ze tot extremen worden opgevoerd. Stuwende beginselen als effectiviteit & efficiëntie verworden in extremis tot economisme, een verankerend beginsel als keuzevrijheid verwordt tot een keuzedelirium en zelfs een procesmatig beginsel als accountability resulteert in excessieve achterdocht en juridisering wanneer daar eenzijdig het zwaartepunt wordt gelegd. Maar ook op het 'middenveld' van de afweging – weg van de extremen – komt het aan op een goede balans. Excessieve nadruk op veiligheid gaat al snel ten koste van privacy en transparantie. Maar een excessieve nadruk op privacy kan ook ten koste gaan van transparantie en accountability, aangezien verantwoording ook altijd een zekere mate van openbaarheid nodig heeft. Bij te veel initiatieven heeft het aan een daadwerkelijke, zorgvuldige en toetsbare afweging tussen deze ongelijksoortige beginselen ontbroken. De bestaande afwegingen – zoals die bijvoorbeeld zijn te vinden in parlementaire stukken – zijn veelal gefragmenteerd en/of obligaat.

Dat ligt uiteraard niet alleen aan de aard van de beginselen zelf. De beginselen moeten ter hand worden genomen op verschillende momenten, op een variëteit aan niveaus en in de vele processen die tezamen resulteren in de iOverheid: in het parlementaire debat over een nieuwe toepassing, in het formuleren van de opdracht aan een ontwikkelaar van een toepassing, in de beslissing om bestanden te koppelen of om nieuwe organisaties op een netwerk aan te sluiten en in de uitspraken van rechters, toezichthouders en burgers over nieuwe ontwikkelingen en genomen besluiten. Op al die momenten staat er veel op het spel en wordt het gewicht van een

enkel beginsel soms zwaar aangezet om het pleit te beslechten. Het empirisch materiaal laat zien dat het bij de ontwikkeling van de iOverheid meerdere malen is voorgekomen dat plannen voor een nieuwe toepassing werden gepresenteerd op manieren die het meest weg hadden van marketing. Technovertrouwen is soms niet zozeer echt vertrouwen, maar eerder een politieke verkoopmethode. Met termen als effectiviteit & efficiëntie en veiligheid zou wel iets minder magie mogen worden bedreven. Maar ook aan de andere kant van het spectrum, aan de zijde van de verankerende noties van privacy en keuzevrijheid, worden reële en toetsbare argumenten en afwegingen vaak evenzeer gemist. Als er aan deze kant iets ingeleverd moet worden – hetgeen zich zeer wel voor kan doen –, dan is het zaak dat deze 'incassering' als zodanig wordt erkend en gecommuniceerd. Met andere woorden, hoewel in de meeste gevallen niet op voorhand te zeggen is wat de 'juiste' inhoudelijke afweging is tussen de stuwende en verankerende beginselen, dient het debat op dit punt wel degelijk sterk verbeterd te worden.

Het realiteitsgehalte van de discussies over de verdere ontwikkeling van de iOverheid, en de rol die de beginselen daarbij spelen, moet drastisch omhoog, omdat het zowel bij hen die wijzen op de kansen als bij hen die wijzen op de gevaren daarvan ontbreekt aan een goede verantwoording van hun zaak. Hierbij is een belangrijke rol weggelegd voor de procesmatige beginselen van transparantie en accountability. Juist een stevige en geloofwaardige invulling van de procesmatige omlijsting van de iOverheid kan bijdragen aan de realiteitswaarde van de discussies die bepalen welke richting moet worden ingeslagen. Evengoed is het noodzakelijk dat de verankerende beginselen expliciet en zoveel mogelijk toetsbaar worden gemaakt. Realiteitszin aan deze kant van het spectrum zou vooral laten uitkomen dat beginselen als privacy en keuzevrijheid geen alles-of-niets-karakter hebben. Het is soms noodzakelijk om op deze beginselen iets in te leveren, mits dit expliciet en goed verantwoord gebeurt. De overheid mag immers ook geen mogelijkheden laten liggen om met behulp van moderne technologie en wetenschappelijk onderbouwde mogelijkheden van risicotaxatie, diagnose en interventie mensenlevens te beschermen (Buruma 2011). Een teveel aan privacy kan een kind in grote moeilijkheden buiten het gezichtsveld van de autoriteiten houden, een teveel aan keuzevrijheid kan in een dusdanig complexe situatie erin uitmonden dat de burger uiteindelijk toch met lege handen staat.

Het expliciet en zo veel mogelijk toetsbaar maken van de stuwende beginselen zou op zijn beurt vooral twee zaken laten uitkomen en dus ook openlijk bespreekbaar maken. Ten eerste, dat vaak sprake is van ongefundeerd politiek-bestuurlijk optimisme ten aanzien van de mogelijkheden van ICT, zoals het empirisch materiaal in dit rapport en vele studies die dit rapport zijn voorgegaan, hebben laten zien. Hoewel optimisme de motor is van veel innovatie, is het in Nederland ook de onderliggende reden geweest voor ondoordachte projecten, onhaalbare deadlines en kostbare ICT-mislukkingen. Ten tweede zou explicitering duidelijk maken dat

'verrommeling' vaak stilletjes is ingecalculeerd. *Spill over* en *function creep* worden in politieke discussies op gepaste afstand gehouden en formeel verworpen, in het volle besef dat de toekomst met een grote mate van waarschijnlijkheid precies datgene zal brengen wat op dat moment van regeringswege formeel wordt uitgesloten. Het formele argument is dan dat de politieke verantwoordelijkheid slechts reikt tot het voorliggende voorstel en niet tot de mogelijkheden die daarin – impliciet, maar eenvoudig voorstelbaar – voor de toekomst besloten liggen. In een iOverheid, die ontstaat uit een aaneenschakeling van dit soort geïsoleerde besluiten is een dergelijke 'na ons de zondvloed' redenering onhoudbaar. Het werkelijke besef 'een iOverheid te zijn' vereist dat de politiek de digitale variant van 'regeren is vooruitzien' serieus neemt en toepast op de impliciete, maar voorzienbare toekomstige ontwikkelingen van informatisering. De overheid neemt in haar beleid vaker een voorschot op de toekomst en het zou haar sieren om dat in de politieke afweging ook, en met een open vizier, te doen.

9.2 WAARSCHUWINGSVLAGGEN VOOR DE iOVERHEID

Het is van belang dat de overheid bij de verdere informatisering een aantal kenmerken van informatie veel bewuster dan nu het geval is in acht neemt. Daarbij gaat het niet, zoals vaak gebeurt, om een inhoudelijke karakterisering van informatie waarbij bijvoorbeeld DNA-gegevens een hogere bescherming vereisen dan biometrische gegevens, die weer een hogere bescherming vereisen dan eenvoudige persoonsgegevens als naam, adres en woonplaats. Hoewel dergelijke onderscheidingen in type gegevens van belang zijn – en in de bestaande wet- en regelgeving deels ook in belangrijke mate zijn verankerd –, verlegt dit rapport de blik liever richting *processen* van informatieverwerking en -gebruik, juist omdat die processen van grote invloed zijn op het karakter en de betrouwbaarheid van de informatie waarop de iOverheid draait en waarvan ze afhankelijk is. Deze processen hebben in het huidige digitale tijdperk een aantal karakteristieken die expliciet in overwegingen en beslissingen meegenomen moeten worden om de iOverheid evenwichtig uit te kunnen bouwen of te beperken.

Aan drie, onderling gerelateerde, processen worden daarom waarschuwingsvlaggen meegegeven. Die waarschuwing is niet bedoeld als een 'verbod', maar bedoeld om de alertheid van beleidsmakers en politici te verscherpen. Het algemene besef 'een iOverheid te zijn' krijgt mede handen en voeten met de waarschuwingsvlaggen: wanneer informatie onderdeel dan wel resultaat is van deze processen dient de overheid alert te zijn op de kwaliteit van de informatie en op de vraag wie de verantwoordelijkheid voor de informatie draagt. In sommige gevallen moet mogelijk ook worden nagedacht over – het stellen van – grenzen aan informatiegebruik. Deze informatieprocessen verlangen expliciete aandacht als het gaat om een gebalanceerde verdere ontwikkeling van de iOverheid. De drie ontwikkelingen die deze drie vlaggen dragen zijn de volgende:

1 Het *vernetwerken* van informatie, i.e. het gezamenlijk gebruik en beheer van informatie in een netwerk van actoren.
2 Het *samenstellen en verrijken* van informatie, i.e. het creëren van nieuwe informatie en profielen op basis van verschillende bronnen uit verschillende contexten.
3 Het voeren van *preventief* en proactief beleid op basis van informatie, i.e. het actief beoordelen van en ingrijpen in de samenleving op basis van informatiegestuurde risicocalculatie.

Deze drie informatieprocessen vormen de kern van de iOverheid en stellen haar in staat om beleid te verfijnen, op maat te snijden, een omvattend beeld te verkrijgen van burgers en beleidsproblemen en daar waar nodig proactief op te handelen. Tegelijkertijd zijn het ontwikkelingen die van invloed zijn op informatie zelf: op het karakter, de betrouwbaarheid, de kenbaarheid, de contextualiteit en herleidbaarheid van informatie. Dat levert niet als zodanig onoverkomelijkheden of fundamentele bezwaren op. Het is wel van belang dat deze processen voldoende worden verdisconteerd in de omgang met, het gebruik van en de verantwoordelijkheid voor die informatie. Daaraan ontbreekt het vaak in de onbewuste iOverheid. Veel meer dan nu het geval is, dient het besef door te dringen dat het juist deze drie ontwikkelingen zijn die grote gevolgen hebben voor (a) de *inhoudelijke* kwaliteit van informatie en (b) voor de eisen aan de *organisatorische* inbedding van informatiestromen. Hieruit volgt een aantal belangrijke randvoorwaarden voor de verdere ontwikkeling van de iOverheid.

9.2.1 INHOUDELIJKE KWALITEIT VAN INFORMATIE

Alle drie de ontwikkelingen – vernetwerken, samenstellen en verrijken van informatie als ook informatiegestuurd preventief en proactief beleid – vereisen een scherpe en kritische blik op zowel kwaliteit als relevantie van de informatie die uit de systemen van de verschillende overheden rolt. In deel II is gewezen op tendenties en reflexen zoals het onbezorgd koppelen van informatiebestanden, het habitueel overschrijden van domeinafbakeningen zoals service, care en control, het zonder een duidelijk vooropgezet plan laten uitdijen van de zee van informatie, de voortdurende verwatering van informatie als gevolg van hergebruik op hergebruik, en ten slotte het stapelen en vermengen van alle soorten informatie. Binnen de iOverheid zoals die in de afgelopen jaren is ontstaan, gaat samengestelde informatie in netwerken eenvoudig over 'grenzen' heen. Dat geldt niet alleen voor de fysieke grenzen tussen nationaal en internationaal, maar in het bijzonder voor het onderscheid tussen publieke en private sectoren en 'hun' informatie, en voor het onderscheid tussen informatie gebruikt voor service, care en control. Bovendien wordt veel van deze informatie eerst gedecontextualiseerd wanneer het uit de oorspronkelijke informatieomgeving wordt gehaald en vervolgens gehercontextualiseerd wanneer het wordt gecombineerd met andere gegevens in een andere

beleidscontext. Dat heeft uiteraard gevolgen voor de betrouwbaarheid en de kenbaarheid van informatie. Dat geldt voor de professionals die met deze gegevens moeten werken (en informatie uit een andere professionele context moeten interpreteren) en wordt nog versterkt wanneer het gaat om informatie die het resultaat is van technische bewerkingen, zoals profiling en data mining. Naarmate data- en informatiebestanden vervuilder zijn – en ze zijn vaak vervuild of vatbaar voor vervuiling – zorgen netwerken er bovendien voor dat de risico's die samenhangen met de (verspreiding van) vervuilde informatie exponentieel groeien. Een vervuilde informatiehuishouding komt immers niet vanzelf tot stilstand. Integendeel. Vaak is eenvoudigweg niemand zich bewust van het kwaliteitsverlies van informatie en volgt bewerking op bewerking en hergebruik op hergebruik. Deze onwetendheid geldt zowel voor de betrokken overheidsfunctionarissen als voor de burgers in kwestie. Het gebrek aan kwaliteit van informatie onttrekt zich, juist in vernetwerkte situaties, maar al te gemakkelijk aan het zicht, zonder dat hiervoor altijd direct een 'schuldige' is aan te wijzen. Eerder is dit een onvermijdelijk risico van wat als het *multipliereffect* van ICT kan worden aangeduid: niet alleen correcte informatie heeft een enorme omloopsnelheid en effectieve distributie gekregen, maar ook foutieve informatie. De administratieve werkelijkheid en de 'werkelijke werkelijkheid' kunnen in de iOverheid veel sterker uiteenlopen dan voorheen, en fouten kunnen zich bovendien veel sneller verspreiden, waarna ze vervolgens veel moeilijker te herstellen zijn. Die fouten hebben in het dagelijkse leven soms grote gevolgen voor individuele burgers. Zeker als op basis van de foutieve gegevens via profilering verrijking van informatie plaatsvindt of proactief beleid wordt gevoerd.

De kwaliteit van de iOverheid vereist dus voortdurend rijksbrede aandacht en beleid. Over de hele linie moet de assumptie dat informatie juist is vervangen worden door het besef dat de informatie op onderdelen hoogstwaarschijnlijk niet accuraat, verouderd en soms zelfs misbruikt en gemanipuleerd zal zijn. Nu is de *default*-positie bij de overheid te sterk dat het systeem de waarheid in pacht heeft, worden de foutmarges genegeerd en verschuift de verantwoordelijkheid voor het probleem steeds meer richting burger. Men is zich onvoldoende bewust van de gevolgen van de iOverheid: het *multipliereffect* en de voortdurende decontextualisering vanwege de netwerken worden niet meegenomen in het bepalen van de kwaliteit van informatie. Of men staart zich juist blind op de positieve gevolgen van netwerken en samengestelde informatie. De aandacht voor de kwaliteit van informatie mag zich niet beperken tot de informatie zelf, maar moet zich ook op de metagegevens richten. Metagegevens zijn de onmisbare wegwijzers in de informatiehuishouding. Ze spelen een cruciale rol bij zowel het traceren van informatie als het duiden van de oorspronkelijke context en herkomst van deze informatie. De kwaliteit van een informatiehuishouding van de iOverheid staat of valt kortom met de aanwezigheid van kwalitatief goede metagegevens. Aandacht voor de kwaliteit van informatie vereist ook gedegen aandacht voor technische en organi-

satorische randvoorwaarden zoals beveiliging, werkprocessen en een betrouwbare authenticatie- en identificatie-infrastructuur.

Het vertrouwen in technologie moet veel beter dan nu het geval is worden afgezet tegen de empirische zekerheid dat alle systemen en informatiestromen naast bedoelde ook onbedoelde effecten sorteren die daarmee ook hun weerslag hebben op de inhoud van de informatie als zodanig. Te vaak houdt de overheid nog sterk – en vaak formeel – vast aan de juistheid van haar gegevens. Anders gezegd: de overheid heeft een te groot vertrouwen in de kwaliteit van informatie en een gebrek aan wantrouwen waar het de kwetsbaarheid van de iOverheid aangaat.

Een bewuste iOverheid benadert de eigen informatiehuishouding voortdurend vanuit een kritische houding. Deze houding kenmerkt zich door een realistisch wantrouwen ten opzichte van de kwaliteit van zowel informatie als informatieprocessen, waarbij beide constant op waarde worden geschat en waar nodig verbeteringen worden doorgevoerd.

De rol die informatie speelt in beleidsprocessen verandert onder de condities van digitalisering. Informatie wordt steeds meer ingezet om een voorschot te nemen op de toekomst en die ontwikkeling breidt zich bovendien verder uit over de terreinen van service, care en control. De klassieke variant daarvan, het gebruik van statistiek om het beleid te informeren en te verbeteren, wordt in toenemende mate aangevuld met een informatiegestuurd beleid dat zich toelegt op het voorspellen van *individueel* gedrag. Informatie en calculatie moeten bijvoorbeeld voorspellen welk kind gevaar loopt en welke reiziger een terrorist zal blijken. Op basis van die risicocalculatie wordt vervolgens gehandeld. De verschuiving naar individueel gedrag betekent dat de opbrengst potentieel zeer hoog is – er wordt een leven gered of een aanslag verijdeld –, maar betekent tegelijkertijd dat de repercussies als die inschatting fout blijkt te zijn ook zeer hoog zijn. Wie onterecht als potentieel terrorist, crimineel of falende ouder in de systemen en netwerken van de overheid wordt opgenomen zal daar de gevolgen van voelen in zijn dagelijkse leven. Het besef dat statistiek en kansberekening worden gebruikt voor individuen, en niet voor brede beleidscategorieën, en de potentiële gevolgen daarvan is zwak ontwikkeld bij de overheid.

De meest pregnante voorbeelden, met de meest verstrekkende gevolgen, zijn te vinden in de domeinen van de (staats)veiligheid en in die delen van de zorg waar het om levensbedreigende situaties gaat. Maar ook op minder precaire beleidsterreinen in de dienstverlening en de zorg geldt dat statistische benaderingen en de uitkomsten van vernetwerkte informatieverwerking soms individuele burgers in de verkeerde hokjes plaatsen en daarin vaak langere tijd vasthouden. Bovendien geldt dat deze domeinen onder invloed van informatisering steeds meer in elkaar vervloeien, zodat fouten zich verspreiden en diffuser worden. Ook blijkt in de

dagelijkse praktijk van het informatiemanagement van de overheid het 'vergeten' van informatie – ondanks bewaartermijnen – onder druk te staan. In profielen en netwerken leidt bepaalde persoonsinformatie een hardnekkig bestaan met alle potentiële gevolgen van dien.

Een iOverheid zal dus een scherp oog moeten hebben voor de mogelijke negatieve en soms zelfs schadelijke effecten van informatiegestuurd beleid. Goede procedures om daarmee om te gaan zijn van groot belang voor individuele burgers die in de knel komen. Ook zijn ze van belang voor het in stand houden en versterken van vertrouwen in de iOverheid. Die procedures vragen om een balans tussen de beginselen van accountability en transparantie enerzijds en om een balans tussen de rol en verantwoordelijkheid van de overheid en van de burger anderzijds. Het is daarbij van belang om een onderscheid te maken tussen de burgerrol van *citoyen* (politiek subject) en de burger als individu (juridisch subject). In het eerste geval gaat het om de burger als een productieve *countervailing power* die inzicht zou moeten hebben in de informatieprocessen van de overheid. In het tweede geval gaat het om de burger die toegang moet hebben tot zijn rechten wanneer hij door de overheid onjuist en/of onheus wordt bejegend of vast komt te zitten in de systemen van de iOverheid. Beide rollen vergen een zekere *vigilance* – een combinatie van waakzaamheid en assertiviteit – om een tegenwicht te bieden tegen de uitbreiding van de iOverheid. Dat is echter geen opstelling van burgers die voor lief kan worden genomen, maar één die ondersteuning vraagt in termen van procedures en rechten. Die moeten gevonden worden in praktische uitwerkingen van accountability en transparantie. Algemeen geformuleerd geldt dat voor de burger als *citoyen* transparantie een hoge prioriteit heeft, terwijl voor de burger als individu de hoogste prioriteit bij accountability ligt.

Om burgers in staat te stellen een *countervailing power* te zijn is een zekere openheid van zaken bij de iOverheid nodig. Zonder transparantie en zeker ook inzicht is reëel toezicht onmogelijk. Dat betekent dat de iOverheid meer openheid van zaken moet geven en burgers meer en vooral ook tijdig 'mee moet laten praten en denken' over de verdere ontwikkeling van de iOverheid. Dat moet ze zowel 'uit eigen beweging' doen als in reactie op vigilante burgers en burgerbewegingen die door middel van verzoeken en procedures informatie boven tafel proberen te krijgen. De platitude dat 'wie niets te verbergen heeft, ook niets te vrezen heeft' kan met een knipoog – het is immers ook echt een platitude – wel wat meer op de iOverheid zelf worden toegepast. De burger in de rol van toezichthouder veronderstelt terecht waakzaamheid en assertiviteit bij burgers die echter, even terecht, meer transparantie aan de kant van de overheid zouden mogen verwachten.

Als het gaat om de burger als individu, zeker als die zijn recht zoekt ten opzichte van de staat, is transparantie hoogstens een begin. Met alleen transparantie wordt

de burger immers wel gefaciliteerd, maar ook verantwoordelijk gemaakt om zijn digitale zaakjes goed op orde te hebben, en daar onvermoeibaar over te waken. Dat zou, alleen al in termen van de digitale kloof, een grote ongelijkheid tussen burgers creëren. Bovendien heeft de burger de autoriteit noch de doorzettingsmacht om daadwerkelijk iets blijvend te wijzigen in de vernetwerkte backoffice van de iOverheid. De empirie heeft laten zien dat burgers in de praktijk slachtoffer worden van fouten in de backoffice en machteloos staan om die fouten te corrigeren. Die praktijk moet dus verder uitgewerkt worden met goede procedures voor eindverantwoordelijkheid en een kenbare ingang om verantwoordelijkheid bij de iOverheid neer te leggen. Daarbij moet een evenwicht gevonden worden tussen de verantwoordelijkheid van de burger om onjuistheden aan te (kunnen) kaarten en de verantwoordelijkheid van de overheden om fouten ook daadwerkelijk recht te zetten. Zeker in de meer gevoelige domeinen van care en control (gekenmerkt door een grote winst voor de samenleving bij succes en grote repercussies voor het individu bij fouten) kan het niet zo zijn dat de burger voor (de gevolgen van) de foutieve of verouderde informatie van de overheid opdraait. Kortom, enerzijds is de verantwoordelijkheid van de overheid groot, omdat alleen zij de doorzettingsmacht heeft om fouten in het volledige netwerk van de iOverheid te corrigeren en niet alleen bij het loket waar het probleem is geconstateerd. Anderzijds moet de drempel voor de individuele burger ook niet te laag zijn, aangezien dan relatief (te) gemakkelijk grote inspanningen aan de kant van het bestuur worden gevraagd.

De iOverheid moet investeren in procedures om transparantie (ter ondersteuning van de burger als citoyen) en accountability (ter ondersteuning van de individuele burger als rechtzoekende) te verbeteren. Verantwoordelijkheid en verantwoordingsprocedures binnen de iOverheid zijn momenteel ontoereikend en onvoldoende effectief, en dienen daarom omvattender, explicieter en helderder te worden benoemd en belegd.

9.2.2 ORGANISATORISCHE INBEDDING VOOR DUURZAME EN RECHTVAARDIGE INFORMATIESTROMEN

Het besef 'een iOverheid te zijn' en in het bijzonder de drie waarschuwingsvlaggen van vernetwerken, samengestelde informatie en informatiegestuurd proactief beleid hebben uiteraard ook gevolgen voor de praktische en organisatorische vormgeving van de iOverheid. De inbedding van informatiestromen in de overheidsorganisatie laat in termen van beheer, kwaliteit en waarborgen, ondanks de steeds vaker gebezigde term 'informatiemanagement', nog veel lacunes zien. De ontwikkeling van de iOverheid tot op heden kan in termen van informatie nog te zeer worden gekenschetst als 'veel *flow*, weinig *management*'. De informatie stroomt steeds vrijelijker door de organisatie van de overheid (en daarbuiten), terwijl de randvoorwaarden voor een goed beheer en management van die informatiestromen achterblijven. De omzetting van papieren dossiers en ladekasten in

digitale gekoppelde informatiebestanden biedt immers niet alleen nieuwe kansen, maar zet ook klassieke taken en verplichtingen van de overheid in een ander daglicht. De praktische organisatie en het management van al de informatie die in de databanken en netwerken van de overheid circuleert, is een kwalitatief andere opgave dan die van het papieren tijdperk. Informatiemanagement gaat ook over het functioneren van het 'geheugen' van de iOverheid en dat hapert aan twee kanten. Enerzijds 'dementeert' de overheid en worden zaken vergeten die niet vergeten mogen worden. Anderzijds onthoudt de overheid meer en meer informatie over haar burgers vanuit de gedachte dat het ooit nog van pas kan komen. Het eerste is (onder meer) schadelijk omdat zonder goed geheugen transparantie en accountability onwerkbare beginselen worden. De archieffunctie stelt de overheid in staat haar eigen handelen over te dragen, te traceren, te openbaren en te verantwoorden. Dat is zowel intern, binnen de overheid, als extern, ten opzichte van burgers, van vitaal belang. Archiveren in tijden van digitalisering vraagt echter om een radicaal andere aanpak van het informatiemanagement van de overheid. De Algemene Rekenkamer heeft hier al meerdere malen, en met grote nadruk, op gewezen en daartoe organisatorische handreikingen gedaan.

Tegelijkertijd lijkt de overheid op andere punten niet in staat of onwillig om informatie te vergeten. Het onbeperkt onthouden van informatie is echter ook schadelijk, omdat dit het risico in zich bergt dat burgers zich niet meer aan hun eigen verleden kunnen ontrekken. De overheid is soms niet bij machte om de eigen bewaartermijnen te respecteren en neigt er bovendien naar deze steeds verder op te rekken vanuit de gedachte dat meer informatie ook betere informatie is. Veiligheid en fraudebestrijding zijn daarbij de magische woorden bij uitstek. Er zijn echter ook goede redenen om niet elk deel van het verleden van burgers te betrekken bij het oordeel van de overheid over burgers in het heden of de toekomst. Het werken met 'burgerbeelden' en profielen voedt de informatiehonger van de overheid en maakt bewaren en onthouden een belang op zichzelf. Burgers worden immers veel sterker het product van hun verleden dan ze in het papieren tijdperk waren. 'Eens een dief, altijd een dief' loopt het gevaar een digitale eeuwigheidswaarde te krijgen. Het feit dat het technologisch mogelijk is om persoonsgegevens tot in lengte van dagen te bewaren is nog geen afdoende reden om dat ook daadwerkelijk te doen. Ook hier zal de specifieke context overigens om nadere en soms ook andere afwegingen ten aanzien van bewaren dan wel vernietigen van informatie vragen. Zo zal informatie in het domein van de opsporing bijvoorbeeld soms anders beoordeeld moeten worden dan informatie in het domein van de gezondheidszorg, waar het voor langere tijd bewaren van gegevens van onschatbare waarde kan zijn voor onderzoek en inschattingen van sterfterisico's en erfelijkheid. Op welke wijze gegevens vervolgens bewaard moeten worden, bijvoorbeeld al dan niet geanonimiseerd, is een volgende vraag die ook per categorie bekeken en beoordeeld moet worden. Het gaat er niet om één norm voor het bewaren of vergeten van alle (persoons)informatie te formuleren (het absolute *recht* op verge-

ten), het gaat er juist om dat de overheid hier een goede en beredeneerde afweging maakt die bovendien ook daadwerkelijk in acht genomen wordt.

Het is voor de verdere ontwikkeling van de iOverheid kortom van wezenlijk belang dat er aandacht is voor haar geheugen. De archieffunctie moet zonder meer versterkt worden, wat een radicale omslag in het denken verlangt. Wat de overheid van haar burgers dient te vergeten vereist een openlijke en voortdurende afweging tussen collectieve belangen, zoals die van veiligheid enerzijds en individuele[1] belangen als het recht op vergeving en vergetelheid anderzijds. Een rechtvaardig geheugen verlangt bovendien dat de overheid zich meer dan nu het geval is rekenschap geeft van de risico's die het gebruik van verouderde gegevens met zich mee kan brengen. De regering dient er daarom op toe te zien dat organisaties binnen de iOverheid structureel aandacht hebben voor het belang van vergeten. Organisaties dienen de afwegingen tussen 'bewaren en vergeten' te doordenken, te expliciteren en het resultaat van deze afwegingen ook daadwerkelijk organisatorisch te verankeren. De iOverheid dient hiernaast naar wegen te zoeken om burgers structureel en laagdrempelig te faciliteren bij het verwijderen van verouderde, onjuiste en niet-accurate gegevens.

De iOverheid moet over een effectief, duurzaam, maar vooral ook rechtvaardig geheugen beschikken. Het belang van bewaren en archiveren verlangt een radicale cultuuromslag. Het belang van vergeten moet blijvend worden geagendeerd en vereist een inhoudelijke en organisatorisch verankerde strategie.

9.2.3 'GRENZEN AAN DE GROEI' VAN DE iOVERHEID?

Een onbewuste iOverheid zal de natuurlijke neiging hebben om verder te groeien: 'grenzen aan de groei' komen pas met bewustzijn in zicht. Tot die tijd worden informatieverzamelingen en koppelingen nauwelijks serieus begrensd, vervuilt informatie, sluiten organisaties en informatiestromen niet meer op elkaar aan, raken burgers en bedrijven, maar ook instanties binnen de overheid zelf verstrikt in de datakluwen van de overheid, wordt identiteitsvaststelling een probleem en wordt het voor burgers vrijwel onmogelijk zich te onttrekken aan de informatie die over hen wordt verzameld, bewerkt en uitgewisseld. Zonder een besef van de iOverheid en wat deze betekent voor de verhouding overheid-burger is er weinig reden of gelegenheid om stil te staan bij de groei van het informatiebouwwerk dat de overheid in uitvoering heeft. Ook geeft het weinig reden tot het stellen van vragen: of dit nodig is, of er behoefte aan en noodzaak tot begrenzing is en hoe het zich verder dient te ontwikkelen. Vragen en afwegingen op het niveau van de samenhang van informatiestromen en de gevolgen daarvan blijven liggen, terwijl de constructie van het bouwwerk van de iOverheid doorgaat. Daarmee doet de overheid zichzelf en haar burgers te kort. Bovendien maakt het niet alleen burgers, maar ook de overheid zelf kwetsbaar.

De dagelijkse praktijk van informatieverspreiding en -koppeling en de redelijkerwijs te verwachten claims op eenmaal verzamelde informatie in de toekomst vereisen een bredere afweging die (a) voorbij het concrete beleidsinitiatief kijkt en (b) voorbij het concrete moment van het hier en nu kijkt. Het daadwerkelijk maken van afwegingen op het niveau van de iOverheid doet ook een fundamentelere vraag rijzen: is de iOverheid zoals die is ontstaan ook de iOverheid die we zouden wensen als we haar expliciet en in het volle besef van de samenhang hadden doordacht en ontworpen? Dat betekent daarmee ook dat de vraag op tafel ligt of er grenzen aan de uitbouw van de iOverheid zitten. Waar zitten die grenzen wel? Waar niet? En op basis waarvan wordt dat bepaald?

Deze vragen naar begrenzing hebben ook te maken met een kwetsbaarheid van de iOverheid die zich het best laat illustreren aan de hand van het karakter van het internet. Het fundamenteel ongereguleerde en open netwerkkarakter van het internet maakt het 'sturen' van het internet of het controleren van de informatie die daarop circuleert in de praktijk vrijwel onmogelijk. Iedereen heeft immers toegang tot informatie wanneer die eenmaal op het net is geplaatst. Wat onjuist of ongewenst is, kan worden weggehaald op de eigen site of, na juridische actie, wellicht van de site van een ander, maar is dan vaak al gekopieerd en duikt als 'mirror' ergens anders op. De ontwikkelingen eind 2010 rondom WikiLeaks vormden bij uitstek een voorbeeld van een site die in snel tempo gekopieerd werd, juist omdat overheden en andere belanghebbenden de daarop geplaatste informatie ontoegankelijk wilden maken. Het onstuurbare karakter van het internet en de fundamentele gevolgen daarvan spelen in afgeleide vorm ook voor de iOverheid en wel op twee niveaus. In de eerste plaats voor de iOverheid zelf, dat wil zeggen de interne informatiehuishouding van de overheid. Die informatiehuishouding verschilt van het internet in die zin dat het om een semigesloten systeem gaat en niet een volledig open systeem als het internet. Dat betekent dat het in goede banen leiden van informatiestromen tot op zekere hoogte mogelijk is. De huidige dynamiek binnen de iOverheid zet die (fragiele) 'stuurbaarheid' van informatie echter onder druk. Zowel het vernetwerken van informatie als het laten vervloeien van informatiestromen over de grenzen van het publiek-private heen maakt dat het semigesloten systeem van de iOverheid *intern* steeds meer op het internet gaat lijken. Informatie is steeds meer van iedereen, in plaats van toebehorend aan één organisatie. Dat betekent ook dat het in goede banen leiden van informatiestromen binnen de iOverheid op dezelfde grenzen stuit als binnen het model van internet. Naarmate die ontwikkeling zich doorzet, wordt het problematischer voor de overheid om informatie te kanaliseren, te verifiëren en voor de betrouwbaarheid in te staan.

Naast het risico dat de internetlogica bij de iOverheid 'naar binnen slaat' is er nog een tweede risico, namelijk dat de iOverheid ongewild deel wordt van het internet. Wederom is de WikiLeaks-affaire, zoals die in het najaar van 2010 in alle hevigheid losbarstte, een aansprekend voorbeeld en een voorbode van wat in de

toekomst ongetwijfeld vaker zal gaan gebeuren. Door WikiLeaks kwam de interne informatiehuishouding van overheden ineens op de digitale straten van het internet te liggen: oncontroleerbaar door het vele kopiëren en de snelle migratie van de informatie van *server* naar *server*, van *cloud* naar *cloud*. Inmiddels worden ook lokale varianten gelanceerd die anoniem en vertrouwelijk (overheids)documenten onthullen, zoals opennu.nl.

Alleen Chinese methoden zouden de geest wellicht terug in de fles kunnen krijgen, maar zelfs dat is de vraag. Om van de wenselijkheid daarvan nog maar te zwijgen. Voordat een dergelijk 'lek' van overheidsinformatie naar het internet realiteit wordt, wordt het risico gezien als een kwestie van beveiliging van data en van techniek en beleid om dat te bewerkstelligen. Zodra een lek resulteert in het verspreiden van gevoelige informatie op internet, is er echter geen beleid meer voorhanden, gaan overheden improviseren om de controle terug te winnen, maar dat biedt een weinig verheffende aanblik. De grote druk die de Amerikaanse overheid op service providers uitoefende om WikiLeaks uit de lucht te halen, bracht Amy Davidson van de *New Yorker* tot de vraag of "Lieberman feels that he, or any Senator, can call in the company running the *New Yorker's* printing presses when we are preparing a story that includes leaked classified material, and tell it to stop us. The circumstances are different, but not so different as to be really reassuring."[2] Toch zijn dergelijke lekken juist door digitalisering nagenoeg onvermijdelijk en zullen ook onvermijdelijk vaker voorkomen in de toekomst: de 250.000 pagina's van WikiLeaks waren in papieren vorm nooit op deze manier en op deze schaal uitgelekt. Het is de gecomprimeerde digitale vorm die informatie mobiel doet zijn en lekken van deze omvang mogelijk maakt: in veel van de eerdere geruchtmakende gevallen van informatielekken in onder meer het Verenigd Koninkrijk ging het ook om enorme aantallen persoonsgegevens die op een verloren USB-stick, kleiner dan een aansteker, stonden. Ook de onvermijdelijkheid van lekken naar internet, of dat nu intentioneel is of het gevolg van fouten, slordigheden of grove nalatigheid, maar zeker ook de verdere consequenties die dergelijke lekken met zich meebrengen, zijn redenen om stil te staan bij de grenzen van de groei van de iOverheid.

Hoewel dit rapport de grenzen van de iOverheid niet zal markeren, aangezien dat in essentie politieke keuzes zijn, kan het wel aangeven welke grensgebieden in die afweging betrokken moeten worden. Het gaat hier kortom om de bewustmaking en de aanzet tot een debat over begrenzing en niet om de exacte vaststelling van die grens. De belangrijkste waarde van het rapport *Grenzen aan de groei* van de Club van Rome lag immers ook eerder in het politiek agenderen van de milieuproblematiek dan in de exacte voorspellingen en extrapolaties in het rapport. De afbakeningen die hierboven zijn gegeven kunnen een eerste aanzet zijn voor het benoemen van grenzen: de combinatie van een expliciete afweging van beginselen en het in acht nemen van de waarschuwingsvlaggen dwingt tot nadenken over de

grenzen van de iOverheid. Ook de vermenging tussen service, care en control en de publiek-private vermengingen die ongemerkt heel gewoon zijn geworden, zijn bij nadere beschouwing en vanuit het perspectief van de iOverheid vaak problematisch. Tenslotte vormt de constatering dat het internet een totaal andere informatieomgeving heeft gecreëerd waarbinnen ook de iOverheid heeft te functioneren, alle aanleiding om het karakter van de iOverheid verder te doordenken en daarnaar te handelen. Hier zijn beredeneerde begrenzingen van groot belang. Niet in de laatste plaats om overheden houvast te geven in het bepalen van wat een juiste omgang is met informatie en het delen daarvan met andere (overheids) partijen. Dat is nu vaak onbepaald. Zo besloot de Belastingdienst niet mee te werken aan de informatie-uitwisseling binnen een divers samengesteld samenwerkingsverband van partijen dat door een gemeente was geïnitieerd met het oog op de ontruiming van een woonwagencentrum.[3] De Belastingdienst achtte zich niet gerechtigd om gevoelige informatie te delen met private partijen als elektriciteitsbedrijven, trok als grote zelfstandige overheidsdienst de eigen 'absolute' grens en verliet de tafel. Ook het in hoofdstuk 7 genoemde arrest van de Hoge Raad waarin grenzen werden gesteld aan het opvragen door het Openbaar Ministerie van reizigersgegevens bij Trans Link Systems is een illustratie.[4] Het stellen van dit soort grenzen en het bepalen van kaders voor de verdere ontwikkeling van de iOverheid zou echter niet af mogen hangen van dergelijke bottom-up acties en geïsoleerde rechterlijke uitspraken. Als de Belastingdienst dan wel Trans Link Systems immers wel met de verstrekking had ingestemd, had het proces van gegevensuitwisseling zich geruisloos en zonder nadere discussie verder voltrokken.

Een bewuste iOverheid kan niet zonder een beredeneerde visie op de grenzen van diezelfde iOverheid. Zowel de dynamiek binnen de iOverheid als de dynamiek in de iSamenleving dwingt daartoe: zonder begrenzing zal de overheid uiteindelijk het vermogen kwijtraken om de verdere ontwikkeling van de iOverheid in werkbare banen te leiden.

9.2.4 EEN AGENDA VOOR DE TRANSFORMATIE NAAR EEN BEWUSTE iOVERHEID

Het breed in het denken en de organisatie van de overheid verankeren van het besef 'een iOverheid te zijn' is een urgente opdracht. Deze kan potentieel echter eenvoudig tegen de politieke waan van de dag wegvallen. En dat is gezien wat er op het spel staat een ongelukkige situatie. Om de inhoudelijke aanbevelingen uit de voorgaande paragrafen te kunnen realiseren dient het bestaande bestuurlijk bestel te transformeren naar een bestel dat in staat is om de uitdagingen van de iOverheid te signaleren en op te pakken. Om dit organisatorisch en bestuurlijk vorm te geven is de betrokkenheid van vele organisaties en lagen van de overheid nodig. Daarmee is het niet alleen de regering die in dit rapport direct wordt aangesproken. Oplossingen kunnen echter wel centraal worden *aangejaagd*. Bovendien geldt dat de dynamiek van de iOverheid dusdanig groot is dat er ruimte moet zijn

om snel nieuwe ontwikkelingen en reacties daarop in het denken te kunnen integreren. Het besef 'een iOverheid te zijn' is geen rustig bezit, maar een permanente opgave. Maar juist in een wereld van snelle en dynamische informatisering is het van belang om ankerpunten in te richten die (a) hoeder zijn van het besef 'een iOverheid te zijn' en (b) de iOverheid van een duidelijk en daadkrachtig aanspreekpunt en gezicht voorzien.

Het huidige institutionele landschap is niet op het beleggen van die ankerpunten toegerust. De kern van de iOverheid schuilt in de samenhang van informatiestromen en netwerken en juist op dat punt geldt dat er geen organisaties zijn die zich om het geheel (kunnen) bekommeren. Het politieke debat is verkaveld in wetten, beleidsterreinen, Kamercommissies en technieken, maar beziet informatie zelden in samenhang, laat staan met het oog op verwevenheid, toekomstige verwevenheden en de gevolgen daarvan. Dezelfde verkokering geldt voor de financiële stromen die met digitaliseringsprojecten verbonden zijn en daarmee ook de mogelijkheden voor aansturing en beïnvloeding daarvan. Er is geen 'ministerie van' of 'Kamercommissie voor Informatie'. Departementen, uitvoeringsorganisaties en lagere overheden bekommeren zich primair om hun eigen beleidsproblemen en hebben weinig oog voor de gevolgen van inkomende en uitgaande informatie-stromen die verder reiken dan de 'grenzen' van hun eigen taak en organisatie. Eenzelfde beeld valt in een grensoverschrijdende context waar te nemen. In Europa wordt het netwerk van informatiestromen en persoonsgegevens steeds verder uitgebouwd en vertakt zonder een open discussie over de vraag of, op welke manier en onder welke voorwaarden Nederland wil aansluiten op een iEuropa in aanbouw. Uitvoeringsorganisaties gebruiken de informatie die ze krijgen in het contact met de burger, maar zijn niet bij machte om fouten in informatiestromen te traceren en voor de gehele keten of het netwerk op te lossen als burgers vastlopen. De vele toezichthouders, zoals het CBP en de Nationale Ombudsman, en meldpunten als het Meldpunt Identiteitsfraude, die sommige uitwassen van de iOverheid voor burgers en overheid benoemen en proberen op te lossen, hebben daar vaak niet de taakopdracht voor (te weinig omvattend) en zijn in de praktijk ook niet in staat (structurele) oplossingen te leveren. Daar waar via programma's en andere arrangementen departementsoverstijgend wordt samengewerkt, zoals binnen het beleidsprogramma Versterking Identiteitsketen Publieke Sector (VIPS), is dat slechts op tijdelijke basis en lang niet altijd op voldoende hoog ambtelijk niveau opgehangen. In alle gevallen ontbreekt het aan doorzettingsmacht om de aanpak en oplossingen over de grenzen van de departementen en instanties heen permanent door te voeren. Het ontbreekt de overheid ook aan de juiste kennis op het snijvlak van beleid en techniek om nieuwe systemen 'iOverheidsproof' te ontwikkelen. Op al deze niveaus worden soms dappere pogingen ondernomen om het geheel van de iOverheid in ogenschouw te nemen, te beoordelen en naar oplossingen voor problemen te zoeken. Maar voor alle bestaande organisaties en arrangementen geldt dat hun wettelijke taak en het

gebrek aan doorzettingsmacht simpelweg niet aansluiten op de uitdagingen van de iOverheid. Vandaar de dringende noodzaak voor een agenda voor institutionele transformatie. In navolging van de empirische realiteit moet de overheid zelf in institutionele zin transformeren van een eOverheid naar een iOverheid. De overheid heeft instituties nodig die haar in staat stellen om de discussie over de verdere ontwikkeling van de iOverheid in goede banen te leiden, om verantwoordelijkheid te nemen voor de eigen genetwerkte informatiehuishouding en burgers te voorzien van bescherming die is geënt op de kenmerken van de iOverheid.

Om de doelen voor de iOverheid handen en voeten te geven, is een institutionele transformatie nodig die drie functies bij de overheid belegt en verankert.

1 De *strategische functie*, i.e. het waarborgen van een weloverwogen verdere ontwikkeling van de iOverheid.
2 De *maatschappelijke functie*, i.e. het versterken van de transparantie van de iOverheid voor burgers en het versterken van de accountability van de iOverheid ten opzichte van burgers die in informatienetwerken verstrikt raken.
3 De *operationele functie*, i.e. het verbeteren van de weloverwogen aansluiting tussen beleid, uitvoering, technologie en informatiestromen en netwerken. Het verbeteren van het opdrachtgeverschap van de overheid.

Deze drie functies vormen de absolute ondergrens van wat nodig is om het besef van de iOverheid vorm te geven en te handelen naar de consequenties die de nieuwe realiteit met zich meebrengt. In de volgende paragraaf worden specifieke voorstellen gepresenteerd die de drie functies voorzien van de noodzakelijke 'institutionele tanden'. Daarbij moet worden opgemerkt dat een solide verankering van de doelen en het daadwerkelijk faciliteren van de uitvoering daarvan uiteindelijk belangrijker is dan het naambordje van de organisatie die figureert in de voorgestelde institutionele uitwerkingen.

De iOverheid noodzaakt tot een transformatie van het bestuurlijk bestel, waarbij bestaande arrangementen op het strategische, maatschappelijke en operationele niveau opnieuw moeten worden ingericht.

9.3 INSTITUTIES VOOR DE iOVERHEID

Het is zeker niet zo dat de iOverheid zoals die zich in de afgelopen jaren heeft ontwikkeld, wordt gekenmerkt door een gebrek aan instituties. In deel II van dit rapport is een bonte stoet van overheidsorganisaties de revue gepasseerd. Een minstens even groot aantal organisaties dat zich bezighoudt met verschillende aspecten en elementen van informatisering en overheid is daarbij niet eens genoemd. Al deze instituties en organisaties kwijten zich zo goed als ze kunnen van hun opdracht op hun eigen specifieke terrein. Het probleem met deze instituties is dat zij, net zoals de iOverheid goeddeels onbewust is ontstaan, voor een

groot deel onbewust met die ontwikkeling zijn meegegroeid of gaandeweg aan het palet zijn toegevoegd. Net zoals de iOverheid is ontstaan door toepassing op toepassing en koppeling op koppeling te stapelen, is het institutionele landschap gegroeid in het licht van individuele toepassingen en de kansen en problemen die zich daarbij voordeden. Het zijn echter de instituties van de eOverheid. De onderlinge samenhang en verwevenheid die kenmerkend is voor de iOverheid is nergens institutioneel belegd. Dat geldt zowel voor de ontwikkeling als het toezicht en handhaving. Ondanks het feit dat vele organisaties vol overgave staan voor de kansen van informatisering of aandacht vragen voor de nadelen en gevaren daarvan: hun handelen blijkt niet krachtig genoeg in z'n geheel. De samenhang wordt nauwelijks gezien, laat staan dat het in de opdracht en het handelen van verschillende organisaties is meegenomen.

Een belangrijke consequentie van de boodschap van dit rapport is dat de iOverheid zich, vanwege haar netwerkkarakter, zeer moeilijk centraal laat aansturen. Hiërarchieën en netwerken vormen een ongemakkelijk huwelijk. Tegelijkertijd zal iets of iemand het besef moeten aanjagen, hetgeen een centrale actor met doorzettingsmacht impliceert. Er zal dus een institutionele verbinding gezocht moeten worden tussen netwerken en beslissingsmacht, zowel binnen de overheid als in verbinding met de bredere maatschappelijke context van de iOverheid. De iOverheid functioneert tegen de achtergrond van een iSamenleving die door informatisering wordt beïnvloed en deze op haar beurt zelf beïnvloedt. Bovendien vloeien de publieke informatienetwerken van de overheid aan de randen vaak over in de private netwerken van bedrijven en burgers. De iOverheid kan niet eigenstandig en in een isolement worden vormgegeven. Het heeft daarbij alle relevante actoren te betrekken – dus behalve verschillende niveaus binnen de overheid, zeker ook de private sector en burgers. Het credo zou moeten zijn: 'Betrek de iSamenleving bij de duurzame uitbouw van de iOverheid.'

Wanneer de boodschap van dit rapport tot zijn uiterste consequentie wordt doorgeredeneerd, is de enige echte institutionele aanbeveling dat het besef 'een iOverheid te zijn' moet inzinken in alle organisaties van de overheid en op alle vitale momenten in het proces van informatisering: vanaf de eerste plannen op nationaal of internationaal niveau, de prille gedachten over een nieuwe applicatie, via een concrete opdracht of aanbesteding tot het koppelen van informatie in een later stadium. De iOverheid moet indalen als een breed verankerd besef. Dat is het gewenste toekomstbeeld. Het ontwikkelen van dat besef zal een evolutionair proces zijn dat mogelijk versneld wordt door externe schokken – de ophef over de publicatie van vertrouwelijke overheidsdocumenten via WikiLeaks of een groot schandaal rondom informatiebeheer, zoals voorbeelden in het buitenland wel hebben laten zien. Maar het ontwikkelen van het besef kan ook door het instellen van instituties die een aanjagende functie hebben. Wat dat betreft is de ambitie van het kabinet-Rutte om een nationale toezichthouder in te stellen voor het

melden van datalekken bij de overheid, een duidelijke stap in de richting die de WRR bepleit (Regeerakkoord 2010: 42). Maar de opgave voor iOverheid reikt verder dan alleen een toezichthouder voor datalekken.

In deze laatste paragraaf van dit rapport worden bij wijze van voorbeeld de contouren geschetst van een viertal instituties die deze aanjagende functie kunnen vervullen. De strategische, maatschappelijke en de operationele functie worden op die manier belegd bij een viertal nieuwe organisaties die in staat moeten worden gesteld om de transformatie naar een iOverheid gestalte te geven. De institutionele voorstellen zijn realistische opties, maar zijn ook een middel om de urgentie van hetgeen gedaan moet worden te expliciteren en uit te werken. Zoals eerder gezegd is de urgentie, en de agenda die daaruit voortvloeit, daarbij belangrijker dan de specifieke uitwerking. Het beleggen van strategische, maatschappelijke en de operationele functies, en deze van zowel middelen als doorzettingsmacht voorzien, heeft de prioriteit. Tegen deze achtergrond worden vier voorstellen voor institutionele innovatie voor de iOverheid gedaan. De strategische functie wordt belegd bij een permanente commissie voor de iOverheid die rapporteert aan de Eerste en Tweede Kamer. De maatschappelijke functie wordt uitgewerkt in een nationaal iPlatform en een iAutoriteit die verantwoordelijk zijn voor de transparantie respectievelijk de opname en afhandeling van problemen van burgers met de iOverheid. De operationele functie wordt uitgewerkt in een organisatie waarin het opdrachtgeverschap van de overheid professioneel belegd kan worden.

9.3.1 PERMANENTE COMMISSIE VOOR DE iOVERHEID

Het besef van de iOverheid moet centraal belegd worden, omdat dit perspectief anders dreigt weg te zakken tussen de specialismen van de verschillende actoren en organisaties die zich met informatisering en gevolgen daarvan bezighouden.

Stel een permanente commissie voor de iOverheid in die jaarlijks aan het parlement rapporteert over de 'staat van informatie'.

De centrale taak van deze commissie is om ontwikkelingen te signaleren, met elkaar in verband te brengen, en te doordenken vanuit het perspectief van de iOverheid, dat wil zeggen over grenzen van departementen en overheidslagen heen en in het perspectief van de mogelijke toekomstige ontwikkelingen. Daarbij gelden de eerder gepresenteerde waarschuwingsvlaggen – bij netwerken, samengestelde informatie en preventief en proactief beleid – als specifieke aandachtspunten bij de advisering. Het jaarlijkse rapport is openbaar en doet aanbevelingen over de voorgenomen plannen van de overheid bezien vanuit het licht van informatie (in tegenstelling tot techniek) en tevens bezien vanuit het bredere perspectief van ontwikkelingen binnen de iOverheid en de iSamenleving. Waar daar aanleiding toe is, moeten internationale ontwikkelingen expliciet in de advisering

betrokken worden. Met name op het internationale en het Europese vlak geldt dat beslissingen worden besproken en genomen die pas veel later zichtbaar worden in de Nederlandse politieke en maatschappelijke arena. Omdat deze beslissingen echter wel bepalend zullen zijn voor de verdere ontwikkeling van de iOverheid en haar vertakkingen over de grenzen van Nederland heen, is het van groot belang deze tijdig te signaleren, bespreken en doordenken. De commissie kan in de advisering tevens invulling geven aan de ambitie van het kabinet-Rutte om voorgenomen maatregelen inzake opslag, koppeling en verwerking van persoonsgegevens al bij de voorbereiding nadrukkelijk te toetsen aan effectiviteit (Regeerakkoord 2010: 42). Het zal daarbij juist de opdracht van de commisssie moeten zijn om deze taak op te vatten vanuit het bredere perspectief van ontwikkelingen binnen de iOverheid en de iSamenleving. Overigens zal de toets meer moeten omvatten dan effectiviteit, maar een afweging zijn van de stuwende, verankerende en procedurele beginselen.

Maar de agenda van de commissie zal breder moeten zijn dan uitsluitend advisering over voorgenomen maatregelen. Een regelmatig terugkerend agendapunt is de evaluatie van lopende, gestrande en afgeronde ICT-projecten in het licht van informatiestromen en de verhouding tussen service, care en control. Juist omdat de iOverheid zich kenmerkt door doorlopende processen van verknoping en vertakking, is het van groot belang om projecten en koppelingen van informatie kritisch te volgen, lessen uit het verleden te trekken en het debat daarover te faciliteren. Dat debat zou dan onder meer moeten gaan over *function creep*. Daarbij moet aandacht zijn voor *function creep* als inherent kenmerk van innovatie en voor *function creep* in problematische zin, waarbij beide zijden van de medaille overigens soms vervelend dicht bij elkaar kunnen liggen. Ook zou de commissie, op basis van de jaarverslagen van het iPlatform en de iAutoriteit (zie verderop) situaties en systemen waarin burgers (maar ook bedrijven) in moeilijkheden komen, moeten inventariseren om daar op een meer algemeen niveau lessen uit te kunnen trekken en verbeteringen of verslechteringen te kunnen monitoren. Een expliciet aandachtspunt bij de evaluatie van ICT-projecten is het voorkomen van de – maar al te gebruikelijke – blikvernauwing naar de technische en financiële kant van ICT-projecten. De commissie zou zich veel sterker moeten richten op het faciliteren en toetsen van de vraag of een nieuwe applicatie ook daadwerkelijk dat levert, in termen van informatie, wat vanuit de achterliggende beleidsdoelstelling was gevraagd. Vanuit de doelstelling te komen tot een verankering van het besef 'een iOverheid te zijn', is lessen willen trekken vooralsnog belangrijker dan verantwoording laten afleggen.

Het rapport van de commissie wordt in beide Kamers van de Staten-Generaal plenair en in aanwezigheid van de voorzitter van de commissie besproken. Het is aan de Tweede Kamer om conclusies te verbinden aan de aanbevelingen. Het bureau van de Rijks-CIO zou het secretariaat van de Commissie moeten voeren

om zo een institutionele verbinding te creëren tussen het besef van de iOverheid in de regering en in het parlement. Ook zou zo de strategische en toekomstgerichte functie van de CIO binnen de rijksoverheid versterkt kunnen worden.

Het bureau van de Rijks-CIO zou tevens ondersteuning kunnen bieden aan een ten behoeve van de commissie op te richten breed maatschappelijk forum. Dit forum moet vanuit een adviserende rol de verbinding tussen de permanente commissie voor de iOverheid en de iSamenleving faciliteren. Naar voorbeeld van het reeds bestaande – breed samengestelde – Forum Standaardisatie dat momenteel het College Standaardisatie ondersteunt, dient dit op te richten forum de commissie voor de iOverheid te voeden met ideeën, aandachtspunten en oplossingen. In het forum zal een breed scala aan stakeholders en deskundigen moeten deelnemen. Behalve vertegenwoordigers van de verschillende departementen, uitvoeringsorganisaties en gemeenten dienen in dit forum ook deskundigen vanuit de private sector (niet als vertegenwoordiger van een specifiek bedrijf, maar vanuit de specifieke kennis die daarmee aan tafel wordt gebracht), wetenschappers, toezichthouders en 'burgers', in de vorm van maatschappelijke organisaties als de Consumentenbond en mensenrechtenorganisaties te participeren. De commissie-Doctors van Leeuwen stelde al in 2001 een dergelijk orgaan voor onder de noemer 'Platform voor de Elektronische Samenleving' die ten dienste zou staan van een regeringscommissaris (Eenmalige Adviescommissie ICT en Overheid 2001). De regering wees de voorstellen van de commissie indertijd af onder verwijzing naar de coördinerende rol voor ICT van de minister van Grote Steden en Integratie. Die zou een betere verankering bieden, concludeerde de regering in haar officiële reactie. Met die redenering kan echter niet meer worden volstaan. Het perspectief van de iOverheid is een breuk met een overheidstraditie van denken in termen van de eOverheid en vereist een ander geluid dan wat een coördinerend minister kan en vaak ook wil brengen. Bovendien vormen de netwerken van de iOverheid, zowel intern als met externe partijen, en de bewustmaking van de effecten daarvan een agenda die niet tot één departement en zelfs niet uitsluitend tot de overheid beperkt moet worden. De iOverheid kan pas een kwestie van coördinatie worden als dat besef daadwerkelijk en duurzaam verankerd is.

9.3.2 HET iPLATFORM EN DE iAUTORITEIT

Eén ontwikkeling die sterk uit de empirie naar voren komt, is het ontstaan van een enorme 'backoffice' van informatiestromen bij de overheid, die deels ook tot buiten de grenzen van de overheid reikt. De informatie in deze netwerken is, zoals eerder gesteld, in termen van verantwoordelijkheid vaak 'verweesd'. Voor burgers is het soms nagenoeg onmogelijk om incorrecte informatie te corrigeren, terwijl ze in hun interactie met de overheid wel met de gevolgen daarvan worden geconfronteerd. Achter de extreme gevallen van identiteitsfraude die de voorpagina's van de kranten halen, gaan vele gevallen schuil van burgers die de bestandsvervui-

ling van de overheid moeten zien te corrigeren en daarvoor geen eenduidige ingang vinden. Het netwerk van organisaties dat zich het lot van deze burgers aantrekt, is noch dekkend noch berekend op die taak. Sommige initiatieven zijn slechts tijdelijk, voor andere vallen individuele problemen buiten de taak, vele hebben nauwelijks personeel en middelen en geen enkele organisatie heeft daadwerkelijk de doorzettingsmacht om fouten in het achterliggende netwerk te corrigeren. Ook de Nationale Ombudsman moest, in de meest gemediatiseerde zaak van identiteitsfraude, de zaak-Kowsoleea, constateren dat een daadwerkelijke correctie van foutieve informatie onmogelijk bleek.

Maar het 'verweesde' beeld betreft niet alleen incorrecte informatie. Het geldt, zo laat de empirie zien, evenzeer de informatie die de overheid via een rijkgeschakeerd landschap aan websites, e-loketten en webportals naar burgers toe communiceert. Meer en meer is bij deze initiatieven een veelheid aan – soms ook private – partijen betrokken en blijken ze zonder een expliciete democratische legitimatie en besluitvorming te zijn ontstaan. Bij veel van deze nieuwe genetwerkte communicatiemodellen is de formele verantwoordelijkheid voor de beschikbare informatie en communicatie bovendien allesbehalve eenduidig belegd. Het goed organiseren van transparantie en accountability zodat de burger niet de dupe wordt van die elementen van de iOverheid waarop hij noch zicht heeft, noch invloed kan uitoefenen, geeft uitvoering aan de maatschappelijke functie.

Transparantie en accountability van de iOverheid moeten van een duidelijk 'adres' worden voorzien. Er dient daarom voor burgers één platform te komen waar de transparantiefunctie invulling krijgt en één autoriteit waar de accountability wordt belegd.

Net zoals de overheid bij haar dienstverlening streeft naar een één-loketgedachte, zou de overheid ook bij de functies van transparantie en correctie naar één ingang moeten streven. Daarmee zouden ook de her en der over internet verspreide en sterk applicatie- of probleemgerichte overheidsfora zoals burgerservicenummer.nl (voor het BSN), infobsnzorg.nl (voor het EPD), lastvandeoverheid.nl, mijnoverheid.nl en het Meldpunt ID-fraude voor burgers onder één digitaal dak gebracht worden. Het iOverheidsplatform moet een interactief informatiepunt zijn over informatisering in de relatie tussen de burger en de overheid: dit is de transparantiefunctie. Door deze informerende functie moet het burgers allereerst via één eenduidige ingang duidelijk worden hoe zij in de gekoppelde systemen van de iOverheid staan geregistreerd en wie en waarom daar toegang toe hebben. Naar voorbeeld van de toeslagenportal van de Belastingdienst moet de burger hier bovendien zijn gegevens (via tussenkomst c.q. na goedkeuring) zelf via een beveiligde omgeving kunnen muteren en corrigeren – waarbij gewaarborgd moet worden dat ze in het gehele netwerk worden aangepast. Het versterken van de transparantiefunctie met interactiviteit als kenmerkend uitgangspunt dient ook de

emancipatie van burgers. De interactieve gedachte achter het platform sluit daarmee aan bij de bredere tendens in de iSamenleving waarin digitalisering de emancipatoire mogelijkheden van burgers versterkt en van nieuwe impulsen voorziet.

De tweede maatschappelijke functie, die van accountability, heeft een actief karakter en is al eerder bepleit door de Nationale Ombudsman (2009a). De iAutoriteit moet ervoor zorgen dat misrepresentaties van burgers in de backoffice en overige systemen daadwerkelijk worden gecorrigeerd. Hier moet het probleem letterlijk uit handen van de burger genomen worden om het in de ketens en netwerken van de iOverheid recht te zetten en op te lossen. Dit is een radicale centralisatie van het beginsel van accountability. De huidige mogelijkheden om decentraal en via verschillende instanties en toezichthouders fouten te corrigeren die in het netwerk zijn opgenomen, zijn door de jaren heen onvoldoende gebleken. Bij deze iAutoriteit moeten expertise en een persoonlijke behandeling worden gecombineerd met een stevige doorzettingsmacht ten opzichte van de organisaties die het netwerk van de backoffice van de iOverheid bevolken. Die doorzettingsmacht is van groot belang, want als deze ontbreekt, neemt de iAutoriteit simpelweg de gemankeerde positie van de burger over wanneer deze door de verschillende organisaties van het kastje naar de muur wordt gestuurd. Dan is het probleem slechts verplaatst, maar niet opgelost. Overigens moet goed worden doordacht in welke mate burgers toegang hebben tot de iAutoriteit. Enerzijds moet het herkenbaar en laagdrempelig zijn, maar anderzijds zou een te lage drempel het voor bepaalde burgers wellicht te gemakkelijk maken om zand in de machinerie van de iOverheid te strooien[5], aangezien dit model relatief grote inspanningen aan de kant van het bestuur veronderstelt.

Het iPlatform zou op digitaal vlak een uitbouw kunnen zijn van het huidige mijnoverheid.nl. Organisatorisch moet de iAutoriteit als een onafhankelijke partij met doorzettingsmacht worden opgezet. Alle bestaande informerende platforms en operationele organisaties, waaronder ook het Meldpunt ID-fraude, dienen in deze organisaties opgenomen te worden dan wel samen te komen. Het iPlatform en de iAutoriteit publiceren jaarlijks een gezamenlijk rapport waarin verslag wordt gedaan van de werkzaamheden, de resultaten daarvan alsmede de belangrijkste ontwikkelingen en trends.

9.3.3 OPDRACHTGEVERSCHAP GEPROFESSIONALISEERD

Het besef van de iOverheid moet uiteindelijk ook belegd worden op het technische niveau van de ontwikkeling van standaarden, applicaties en koppelingen van informatie. Dit is de operationele functie. Op de tekentafels van de techniek en in de (internationale) gremia van de standaarden wordt immers bepaald hoe de iOverheid er in de praktijk uit komt te zien. Het besef dat dit in essentie politieke en beleidsmatige keuzes zijn, valt in de praktijk vaak weg tegen de gedachte dat

techniek niet meer dan een instrument is. Wie de informatiestromen volgt – zoals in dit rapport is gedaan – weet dat via de techniek categorieën ontstaan en *categories have politics*. Dat betekent dat ontwerpkwesties, standaardisaties en interoperabiliteit allemaal van bepalend belang zijn voor de ontwikkeling van de iOverheid als geheel en niet alleen voor individuele applicaties en beslissingen.
Een van de cruciale momenten in de ontwikkeling van de iOverheid is het opdrachtgeverschap van de overheid. Het uitwerken en vaststellen van de eisen aan en de functies van nieuwe systemen en applicaties is bepalend voor de (toekomstige) mogelijkheden van nieuwe toepassingen en hun plaats in het bredere kader van de iOverheid. De overheid hinkt daarbij sterk op twee gedachten; enerzijds wil zij de ontwikkeling vaak zelf ter hand nemen, bijvoorbeeld via de ontwikkelorganisatie ICTU, anderzijds blijkt het onmogelijk en onpraktisch om de benodigde technische kennis zelf in huis te hebben. Het overgrote deel van de technici 'in dienst' van de overheid zijn externe adviseurs en technici. Het resultaat is een overinvestering in technische kennis, en te weinig aandacht voor de interactie tussen beleid, uitvoering en techniek waarin informatiestromen centraal staan.

Het opdrachtgeverschap van de overheid zou daarom over een geheel andere boeg gegooid moeten worden door te investeren in kennis op het snijpunt van beleid, uitvoering en techniek in plaats van investeren in technische kennis. Wil de overheid het oplossen van de ICT-problemen structureel aanpakken, zoals het kabinet-Rutte ambieert (Regeerakkoord 2010: 42), dan zal het de aandacht moeten verleggen van technische ontwikkeling naar de professionele opdracht. Dat betekent dat de technische realisatie primair aan partijen buiten de overheid wordt overgelaten (door applicaties daar te laten ontwikkelen dan wel op de markt in te kopen). De overheid zelf dient te investeren in de kennis om de opdracht te formuleren, het pakket van eisen en de juridische context en randvoorwaarden scherp te krijgen, een en ander in een bredere context te doordenken en de ontwikkeling vakkundig te begeleiden. Dat de techniek werkt, is de taak van de ontwikkelaar. Dat de techniek de 'juiste' informatie genereert en informatieprocessen faciliteert binnen de categorieën en bandbreedten die in het beleid en in overleg met de uitvoering zijn geformuleerd is de controlerende en begeleidende taak van de opdrachtgever.
Dit betekent dat een organisatie ingericht moet worden die een andere invulling geeft aan het opdrachtgeverschap en daarbij niet gebonden is aan de grenzen van departementen en individuele uitvoeringsorganisaties. Deze organisatie zou een kleine kern hebben van eigen ICT'ers en ICT-juristen met kennis van de iOverheid die per project aangevuld kan worden met de CIO van het betreffende beleidsdepartement, ambtenaren van het beleidsdepartement en medewerkers vanuit uitvoeringsorganisaties die met het uiteindelijke systeem moeten werken. Het structureel betrekken van de ketenpartners of de netwerkpartners bij de ontwikkeling van applicaties lijkt een open deur, maar is in de praktijk relatief zeldzaam. Ook hier lopen de informatiestromen in de regel vooruit op de betrokken organisaties.

De iOverheid dient werk te maken van goed opdrachtgeverschap, waarbij investeren in eigen kennis op het snijpunt van beleid, uitvoering en techniek prioriteit heeft boven het in huis hebben van zuiver technische kennis en ontwikkelcapaciteit.

9.4 DE iOVERHEID IN UITVOERING

Om zowel aan te sluiten bij de realiteit van de iOverheid als in staat te zijn de verdere ontwikkeling daarvan in werkbare banen te leiden zal de Nederlandse overheid in woord en daad de transformatie van een eOverheid naar een iOverheid moeten maken. Wil de overheid in de toekomst het pad van digitalisering met vertrouwen kunnen vervolgen, dan zal het besef 'een iOverheid te zijn' in alle lagen van de overheid verankerd dienen te worden. Daarbij schuilt de belangrijkste inhoudelijke opdracht in de bereidheid en het vermogen het debat niet langer te voeren via de band van technieken en individuele applicaties, maar dit debat aan te gaan vanuit het besef van samenhangende informatieprocessen en verknoopte informatie. Van wezenlijk belang daarbij is allereerst dat er ruimte en aandacht is voor een open afweging tussen de drijvende, verankerende en de procedurele beginselen. Een zorgvuldige ontwikkeling van de iOverheid kan niet zonder een dergelijke afweging, waarbij het van groot belang is dat deze afweging wordt gemaakt in het licht van de iOverheid als geheel. Hiernaast geldt dat van de overheid bij zowel deze afweging als de verdere inrichting van beleid en uitvoering, extra behoedzaamheid verlangd mag worden wanneer sprake is van een drietal in dit rapport gesignaleerde processen van informatieverwerking. Deze processen – die in symbolische zin zijn voorzien van waarschuwingsvlaggen – houden verband met a) het vernetwerken van informatie, b) het samenstellen en verrijken van informatie, en c) het voeren van preventief beleid op basis van informatie. De specifieke gevolgen die deze processen hebben voor de uitvoering van beleid, de positie van burgers, de kwaliteit van de overheidsinformatiehuishouding en de interne en externe aanknopingspunten voor aansprakelijkheid en verantwoording, noodzaken tot behoedzaamheid en een kritische houding ten opzichte van nut, noodzaak en maatschappelijke consequenties van digitaliseringsinitiatieven.

Om deze inhoudelijke opdracht van pleitbezorgers te voorzien en daarmee zorg te dragen voor de noodzakelijke institutionele verankering formuleert dit rapport een agenda voor institutionele transformatie. De instituties die in het kader van deze transformatie worden voorgesteld moeten garanderen dat de iOverheid de instrumenten in handen heeft om bewustwording, bescherming en innovatie te faciliteren. Daarbij moet het overigens helder zijn dat de institutionele transformatie als zodanig vele malen belangrijker is dan de in dit rapport voorgestelde (naambordjes van) instituties. Op een drietal niveaus zal de noodzakelijke transformatie gestalte moeten krijgen. Op het strategische niveau (via de installatie van een permanente commissie voor de iOverheid), op het maatschappelijke

niveau (via een iPlatform ten behoeve van transparantie en een iAutoriteit ten behoeve van accountability) en op het operationele niveau (via professionalisering van het opdrachtgeverschap en prioritering van kennis op het snijvlak van techniek en beleid in plaats van kennis van de techniek zelf). Ten slotte, voor zowel de inhoudelijke opdracht als de noodzakelijke institutionele transformatie geldt dat de ontwikkeling van de iOverheid niet los gezien kan worden van het pad dat de bredere iSamenleving volgt.

NOTEN

1 Uiteindelijk is dat uiteraard ook een collectief belang, omdat een samenleving die niet vergeet en vergeeft een fundamenteel andere is dan een samenleving waarin men opnieuw kan beginnen.

2 Senator Joseph Lieberman had in een statement laten weten dat providers als Amazon (die WikiLeaks had gehost) al hun banden met WikiLeaks dienden te verbreken. "I will be asking Amazon about the extent of its relationship with WikiLeaks and what it and other web service providers will do in the future to ensure that their services are not used to distribute stolen, classified information", zie het artikel Banishing WikiLeaks van Amy Davidson in the New Yorker, http://www.newyorker.com/online/blogs/closeread/2010/12/banishing-wikileaks.html, opgevraagd 10.12.2010.

3 Gesprek met dhr. P. Wijntje en dhr. S. Peereboom (Financiën/Belastingdienst), 19 oktober 2010.

4 LJN: BK6331, Hoge Raad, 08/04524 B.

5 Vgl. de discussies over (m.n.) milieuorganisaties en hun toegang tot de bestuursrechter.

epiloog: de iOverheid en de iSamenleving

In de kern gaat dit rapport over de verantwoordelijkheid van de overheid voor haar eigen gebruik van ICT. Maar de rol en verantwoordelijkheid van de overheid in de informatiesamenleving reiken natuurlijk verder. Behalve de verantwoordelijkheid voor de iOverheid, berust bij de overheid ten principale ook een zekere verantwoordelijkheid voor het functioneren van de iSamenleving. Die bredere verantwoordelijkheid is in de volgende vragen te vatten: 'Wat dient de overheid zich in de ontwikkeling van de informatiesamenleving aan te trekken, en (hoe) heeft zij daarin te interveniëren?' Toenmalig premier Kok kaartte de kwestie al eens aan in een toespraak op het Infodrome-congres op 11 april 2001: "Toch moeten wij ons thans de vraag stellen welke verantwoordelijkheden, in de jaren die voor ons liggen, op de weg van de overheid komen in verband met aan de informatiesamenleving inherente gevolgen." Deze verantwoordelijkheid kan worden gedefinieerd als de systeemverantwoordelijkheid van de iOverheid voor de iSamenleving. Uiteraard zijn de interventies in de iSamenleving altijd politiek gekleurd en omstreden, maar er kan toch worden geprobeerd een soort *common ground* te formuleren voor de zaken waar een overheid garant voor moet staan. De systeemverantwoordelijkheid van de iOverheid kan niet zonder meer terzijde geschoven worden.

Allereerst omdat de overheid moet opkomen voor haar burgers wanneer private partijen het belang van deze burgers onvoldoende garanderen. Zo stelt de groeiende informatiemacht van mondiale spelers als Google, Facebook en Apple de (Europese) overheid voor de vraag of en op welke wijze deze macht om redenen van publieke belangen beteugeld dient te worden. Op een aantal dossiers zijn al eerste bewegingen in die richting waar te nemen. Voormalig minister van Economische Zaken, Van der Hoeven, deed in reactie op Kamervragen begin augustus 2010 de toezegging het College Bescherming Persoonsgegevens (CBP) te vragen om een nieuwe clausule in de privacyvoorwaarden van Apple te beoordelen.[1] Sommige kwesties die aan de systeemverantwoordelijkheid van de overheid raken, zullen echter op Europees niveau en via een Europese actor (*lead authority*)[2] geadresseerd moeten worden, omdat alleen daar de noodzakelijke massa en doorzettingsmacht gevonden kunnen worden. Maar ook de populariteit van interactieve communicatie via sociale netwerken en web 2.0 roept de vraag op of er een verantwoordelijkheid voor de overheid ligt om de gedragingen van burgers te sturen en te beperken en/of burgers te beschermen tegen marktpartijen. Tot op zekere hoogte geldt bovendien dat de systeemverantwoordelijkheid van de overheid voor bovenstaande en andere ontwikkelingen juridisch afdwingbaar is op grond van de mensenrechten (De Hert 2011).

"De aanname dat de Europese rechtspraak te weinig concrete handvatten geeft voor overheden is onterecht. Op het gebied van de bescherming van persoonsgegevens heeft het Hof algemene beginselen ontwikkeld, die in steeds meer zaken toegepast worden. Hetzelfde is in iets mindere mate waar voor de strijd tegen identiteitsfraude en de bescherming van het mediapluralisme. Nederland kan met die beginselen aan de slag" (De Hert 2011).

De vraag *hoe* de iOverheid haar systeemverantwoordelijkheid moet invullen is in die zin wellicht prangender dan de vraag *of* ze die moet invullen.

Ten tweede kan systeemverantwoordelijkheid ook aan de orde zijn wanneer ontwikkelingen in het private domein te zeer interfereren met (vitaal) beleid van de overheid. Illustratief hier zijn de ontwikkelingen op het terrein van identiteitsmanagement. Zoals deel II van dit rapport laat zien, investeert de overheid veel in digitale middelen om de identiteit van burgers vast te stellen, bijvoorbeeld via applicaties als het (biometrisch) paspoort, DigiD en mogelijk in de toekomst het eRijbewijs. Juist omdat de overheid veel investeert in die identiteitsbepaling – en de accuratesse daarvan claimt – moet ze ook aandacht hebben voor identiteitsbepaling in het semipublieke en commerciële domein, in het bijzonder voor de risico's op verwatering van de kwaliteit daarvan. Wat bijvoorbeeld is de waarde van een streng beveiligde centrale opslag van biometrische gegevens in het kader van de Paspoortwet, als dezelfde gegevens ook buiten het domein van de overheid breed beschikbaar zijn? De invoering van een biometrisch paspoort roept vragen op over het gebruik van biometrie in de private sector. Momenteel is nauwelijks sprake van regulering of zelfs maar politieke aandacht en experimenteren zwembaden, supermarkten, werkgevers en computerfabrikanten volop met nieuwe toepassingen van deze technologie.

Vanwege de enorme toename van verzamelde informatie worden identificaties ook buiten de overheid steeds belangrijker als sleutels om informatie te kunnen koppelen en combineren. Het empirisch materiaal laat zien dat bij het gebruik van identificaties de grenzen tussen de publieke en private sector steeds diffuser worden, hetgeen impliceert dat ook de effecten van dat gebruik over de grenzen heen spelen. Zeker nu sommige actoren in de private sector een publiekrechtelijke taak hebben (notaris) dan wel de overheid van private partijen verlangt dat ze de identiteit van burgers vaststelt (Wet identificatieplicht dienstverlening; arbeidsrelatie) aan de hand van door de overheid uitgegeven identiteitsdocumenten. Het BSN bijvoorbeeld werd als identificatiesleutel bedacht voor overheidsdiensten, zonder er rekenschap van te geven dat het zich binnen de kortste keren tot een *universal* (pubiek-private) *unique identifier* zou ontwikkelen. Om deze en andere redenen moet de overheid alert zijn op ontwikkelingen buiten de overheid en overwegen of en wanneer het noodzakelijk is nadere kaders of regels te stellen.

Dat een zekere eindverantwoordelijkheid ten principale bij de overheid ligt wil overigens nog niets zeggen over de vraag of zij die ook zelf ter hand moet nemen (De Hert 2011) of daar zelfs maar de mogelijkheden en capaciteiten voor in huis heeft (Meijer 2011). De grondrechtelijke eindverantwoordelijkheid van de overheid is bovendien een lastige zaak, omdat er voor een aantal valkuilen gewaakt moet worden. In de eerste plaats moet er niet te gemakkelijk over sturing worden gedacht. Interveniëren in maatschappelijke en in dit geval informationele verhoudingen is weliswaar de bestaansreden van de staat, maar het is tegelijkertijd in zekere zin een waagstuk: interventies kunnen door allerlei factoren in hun tegendeel verkeren, en het is zaak daar vooraf bij stil te staan. In de tweede plaats is het een valkuil om interventies met een 'gebruikersmentaliteit' aan te vatten: de informatiesamenleving is niet 'van de overheid', en daarom dient er ten volle rekenschap gegeven te worden van de rechtsstatelijke voorwaarden die aan interventies gesteld worden. In de derde plaats zijn er verschillende manieren om te interveniëren, en zijn verkeerde keuzes snel gemaakt. Om met de meest traditionele modus te beginnen: de overheid kan zich dwingend regulerend mengen in de informationele verhoudingen. Zij kan zich echter ook helemaal aan de 'zachte' kant van het spectrum positioneren door zich enkel als gesprekspartner voor private spelers op te stellen. Daartussenin bevindt zich nog de specifieke modus van het faciliteren: randvoorwaarden scheppen voor het tot ontplooiing komen van maatschappelijke mogelijkheden. Bij deze verschillende modi horen steeds andere verantwoordelijkheidsoverwegingen.

Volgens Meijer (2011) wordt het echter steeds lastiger, en misschien wel fundamenteel onmogelijk, om vanuit systeemverantwoordelijkheid een centrale rol te spelen in de turbulente, complexe, technologische netwerken: "In plaats van een overkoepelende verantwoordelijkheid zal de overheid steeds sterker twee andere verantwoordelijkheden kunnen nemen: een procesmatige verantwoordelijkheid en een restverantwoordelijkheid." Een procesmatige verantwoordelijkheid betekent dat de overheid niet langer de verantwoordelijkheid neemt voor uitkomsten, maar wel voor de kwaliteit van het proces. Vanuit een restverantwoordelijkheid dient de overheid te waarborgen dat de relevante partijen werken aan bescherming van burgers en het voorkomen van systeemfalen: de overheid dient nu ook de taken op zich te nemen die door andere partijen niet worden vervuld. De voorgestelde commissie voor de iOverheid kan in het denken over systeemverantwoordelijkheid van de overheid een belangrijke agenderende rol spelen. De kernvragen die de commissie vanuit deze rol kan adresseren zijn: welke ontwikkelingen in de bredere iSamenleving dienen ondersteund of juist beteugeld te worden en op welk niveau (nationaal of internationaal) kan normerend optreden het beste worden belegd? Van welke ontwikkelingen kan worden verwacht dat de effecten zullen doorsijpelen in de iOverheid en wat betekent dat voor eventueel regulerend (conditionerend) optreden?

Bepaalde ontwikkelingen in de iSamenleving zullen de overheid echter in toenemende mate voor fundamentele vragen stellen waarop momenteel nog geen begin van een antwoord geformuleerd is. De snelheid waarmee informatie – ook als die de overheid onwelgevallig is – wordt verspreid en gekopieerd, maakt dat de overheid ook na zal moeten denken over haar eigen informatiemanagement. Dat heeft de WikiLeaks-affaire overtuigend laten zien. Transparantie wordt in de regel gezien als iets wat de overheid haar burgers gunt (passieve openbaarheid), veel minder als een actief na te streven belang (actieve transparantie) en al helemaal niet als iets wat door (enkele) burgers wordt genomen of afgedwongen. In de digitale wereld zullen overheden zich echter steeds vaker voor de vraag gesteld zien hoe ze met transparantie om willen gaan. John Naughton schreef in *The Guardian* dat overheden voor een keuze staan: "Live with the WikiLeakable world or shut down the net. It's your choice" (Naughton 2010b). Die laatste keuze zal niet snel gemaakt worden. Desalniettemin zal er wel naar een hernieuwde balans tussen informatievrijheid, geheimhouding en beveiliging van gegevens gezocht moeten worden, waarbij regulering mogelijk aan de orde is. Een deel van het antwoord zal gezocht en gevonden worden in regulering van partijen buiten de overheid (servers, clouds enz.), voor een ander deel moet de overheid wellicht bij zichzelf te rade gaan. Sommige informatie moet misschien helemaal niet opgeslagen worden, andere informatiebronnen moeten wellicht juist transparanter in plaats van vertrouwelijk en geheim en sommige informatie moet wellicht nog beter beveiligd worden.[3] Maar de onvoorspelbaarheid en onzekerheid van de samenleving en daarmee ook van de iSamenleving zal de overheid uiteindelijk nooit volledig buiten de deur kunnen houden, zoals de WRR (2008) al eerder betoogde (zie ook Van Asselt et al. 2010).

Als het gaat om de verantwoordelijkheid van de iOverheid voor de iSamenleving geldt eenzelfde soort afwegingskader als voor het gebruik van ICT door de overheid zelf. Het definiëren van een systeemverantwoordelijkheid komt in essentie ook voort uit een afweging van stuwende, verankerende en procesmatige beginselen, zij het dat de stuwende beginselen nu veelal buiten de overheid liggen. Burgers en bedrijven worden voortgestuwd door enthousiasme voor nieuwe technische mogelijkheden en overwegingen van winstgevendheid. Waar deze structureel onvoldoende worden afgewogen tegen verankerende beginselen en onvoldoende in balans worden gebracht met een uitwerking van procesmatige beginselen die informatiestromen voor burgers transparant en, indien nodig, aanvechtbaar maken, dient de iOverheid zich af te vragen of ze aan zet is.

NOTEN

1 Brief van minister van Economische Zaken, beantwoording vragen over nieuwe clausule in de privacyvoorwaarden van Apple, 03-08-2010.

2 Binnen Europa wordt inmiddels gepleit voor een *lead authority* met voldoende bevoegdheden om dit soort zaken voor de 27 lidstaten op te knappen (gesprek J. Hennis-Plasschaert, VVD-fractie Tweede Kamer, 4 november 2010).

3 Zoals onder meer wordt gesuggereerd in de analyse van 'WikiLeaks – cable gate' door Bits of Freedom. Zie Ot van Daalen, De wereld na WikiLeaks' cable gate, op https://www.bof.nl/2010/12/10/de-wereld-na-wikileaks-cablegate/

LIJST VAN AFKORTINGEN

ACTA	Anti Counterfeiting Trade Agreement
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMvB	Algemene maatregel van bestuur
ANPR	Automatic Number Plate Recognition
ANWB	Algemene Nederlandse Wielrijders Bond
AWBZ	Algemene Wet Bijzondere Ziektekosten
BBP	Bruto Binnenlands Product
BKWI	Bureau Keteninformatisering Werk en Inkomen
BPR	Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten
BSN	Burgerservicenummer
CBP	College Bescherming Persoonsgegevens
CBR	Centraal Bureau Rijvaardigheidsbewijzen
CBS	Centraal Bureau voor de Statistiek
CIO	Chief Information Officer
CIOT	Centraal Informatiepunt Onderzoek Telecommunicatie
CIZ	Centrum Indicatiestelling Zorg
CJIB	Centraal Justitieel Incassobureau
CVZ	College voor Zorgverzekeringen
CWI	Centrum voor Werk en Inkomen
DKD	Digitaal Klant Dossier
DNA	Deoxyribonucleic Acid
DPI	Deep Packet Inspection
ECP-EPN	Platform voor de InformatieSamenleving
EDI	Electronic Data Interchange
EDPS	European Data Protection Supervisor
EHRM	Europees Hof voor de Rechten van de Mens
EKD	Elektronisch Kinddossier
ELD	Elektronisch Leerdossier
EMD	Elektronisch Medisch Dossier
eNIK	Elektronische Nederlandse Identiteitskaart
ENTOPOL	Enforcement Police
eOverheid	Elektronische overheid
EPD	Elektronisch Patiëntendossier
EVRM	Europees Verdrag voor de Rechten van de Mens
FCC	Federal Communications Commission
GBA	Gemeentelijke Basisadministratie
GMS	Geïntegreerd Meldkamersysteem
GPS	Global Positioning System
GSD	Gemeentelijke Sociale Dienst
HARM	Hospital Admissions Related to Medication

HEC	Het Expertise Centrum
HKS	HerKenningsdienst Systeem
IB-Groep	Informatie Beheer Groep
ICAO	International Civil Aviation Organization
ICTU	ICT Uitvoeringsorganisatie
IGP	Informatiegestuurde Politiezorg
IMI	Internal Market Information System
IND	Immigratie- en Naturalisatiedienst
ISP	Internet Service Provider
JBZ	Justitie en Binnenlandse Zaken
Kecida	Kennis- en expertisecentrum voor intelligente data-analyse
KLPD	Korps landelijke politiediensten
LIS	Landelijk Informatiesysteem Schulden
MI5	Military Intelligence, Section 5 (VK)
NAW	Naam, Adres, Woonplaats
NORA	Nederlandse Overheids Referentie Architectuur
NUP	Nationaal uitvoeringsprogramma betere dienstverlening en e-overheid
OECD	Organisation for Economic Co-operation and Development
PET	Privacy Enhancing Technology
PIP	Persoonlijke Internet Pagina
PNR	Passenger Name Records
R&D	Research and Development
RAND	Research and Development Corporation
RDW	Rijksdienst voor het Wegverkeer
RFID	Radio-frequency identification
RINIS	Routerings Instituut voor (inter)Nationale Informatiestromen
ROB	Raad voor het openbaar bestuur
SCP	Sociaal en Cultureel Planbureau
SIOD	Sociale Inlichtingen- en Opsporingsdienst
SIS	Schengen Informatie Systeem
SISA	Stadsregionaal Instrument Sluitende Aanpak
SUWI	Structuur Uitvoeringsorganisatie Werk en Inkomen
SVB	Sociale Verzekeringsbank
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UWV	Uitvoeringsinstituut Werknemersverzekeringen
VIPS	Versterking Identiteitsketen Publieke Sector
VIR	Verwijsindex Risicojongeren
VIS	Visum Informatie Systeem
VNG	Vereniging Nederlandse Gemeenten
VNO-NCW	Verbond van Nederlandse Ondernemingen – Nederlands Christelijk Werkgeversverbond
Wajong	Wet arbeidsongeschiktheidsvoorziening jonggehandicapten
WBP	Wet Bescherming Persoonsgegevens

WIA	Wet werk en inkomen naar arbeidsvermogen
WMO	Wet Maatschappelijke Ondersteuning
Wob	Wet openbaarheid van bestuur
Wsw	Wet sociale werkvoorziening

LITERATUURLIJST

Actal (2010) *Brief van 10 mei 2010 Advies ICT-beleid en vermindering regeldruk* (n.a.v. ICT-onderzoek: Uit het Zicht. Beleidsmaatregelen voor het versnellen van het gebruik van ICT-toepassingen voor administratieve lastenverlichting*)*, Den Haag.

Adviescommissie Informatiestromen Veiligheid (2007) *Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse*, april 2007, Den Haag: Deltahage.

Akker, R. van den & M. Kuiper (2008) 'De bureaucraat als dompteur. De domesticatie van de digitale overheid', blz. 153-165 in V. Frissen & J. de Mul (red.) *De draagbare lichtheid van het bestaan*, Kampen: Uitgeverij Klement.

Algemene Inlichtingen- en Veiligheidsdienst (2010a) *Jaarverslag 2009*, Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Algemene Inlichtingen- en Veiligheidsdienst (2010b) *Kwetsbaarheidsanalyse spionage*, Den Haag: AIVD.

Algemene Rekenkamer (1991) *Machineleesbare gegevens. Archivering en beheer bij het Rijk*, Den Haag: Sdu.

Algemene Rekenkamer (1998) *Beheer en archivering van digitale bestanden.* Kamerstukken II 1997-1998, 25970, nr. 2.

Algemene Rekenkamer (2003) *Communicatienetwerk C2000 en Geïntegreerd Meldkamersysteem (GMS)*, Den Haag: Sdu.

Algemene Rekenkamer (2007a) *Lessen uit ICT-projecten bij de overheid*, Den Haag: Sdu.

Algemene Rekenkamer (2007b) *Aanbesteding ICT-Component P-Direkt*, Den Haag: Sdu.

Algemene Rekenkamer (2008a) *Lessen uit ICT-projecten bij de overheid – Deel B*, Den Haag: Sdu.

Algemene Rekenkamer (2008b) *ICT-project huur- en zorgtoeslag*, Den Haag: Sdu.

Algemene Rekenkamer (2009) *Informatiehuishouding van het Rijk*, Den Haag: Sdu.

Algemene Rekenkamer (2010a) *Informatiehuishouding van het Rijk. Overzicht van een dynamisch vraagstuk, een achtergrondstudie,* Den Haag: Sdu.

Algemene Rekenkamer (2010b) *Informatiehuishouding van het Rijk, Stand van zaken juni 2010 fact sheet*, http://www.rekenkamer.nl/Actueel/Onderzoeksrapporten/Bronnen/2010/06/Factsheets_Vooropname/Informatiehuishouding_van_het_Rijk, geraadpleegd op 24 september 2010.

Allen, A. (2003) *Why privacy isn't everything: feminist reflections on personal accountability*, Lanham, MD: Rowman en Littlefield.

Ambtelijke Commissie Toezicht II (2004) *Rapport van Bevindingen betreffende de zelfevaluatie door het College Bescherming Persoonsgegevens (CBP) van het toezicht op de verwerking van persoonsgegevens*, Den Haag, 16 december 2004.

Anders, G. (1980) *Die Antiquiertheit des Menschen. Über die Seele im Zeitalter der zweiten industriellen Revolution*, Munchen: C.H. Beck.

Anderson, C. & M. Wollf (2010) 'The web is dead. Long live the internet', *Wired Magazine*, september 2010, http://www.wired.com/magazine/2010/08/ ff_webrip/.

Andeweg, R. & H. van Gunsteren (1994) *Het grote ongenoegen: over de kloof tussen burgers en politiek*, Haarlem: Aramith.

Article 29 Data protection working party en working party on police and justice (2009) *The future of privacy*, Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09/EN, WP 168.

Attema, J. & D. de Nood (2010) *Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit,* rapportage van ECP-EPN in samenwerking met de WRR, WRR-webpublicatie nr. 47, www.wrr.nl.

Aus, J. (2008) *EU governance in an area of freedom, security and justice. Logics of decision making in the Justice and home affairs Council*, Dissertation, University of Oslo.

Baker, S. (2008) *The numerati*, Boston: Houghton Mifflin.

Balzacq, T. (2008) 'The policy tools of securitization. Exchange, EU foreign and interior policies', *Journal of Common Market Studies* 46, 1: 75-100.

Barney, D. (2004) *The network society*, Cambridge: Polity.

Beck, U. (1992) *Risk society. Towards a new modernity*, London: Sage Publications.

Bekkers,V.J.J.M. (1998) *Grenzeloze overheid. Over informatisering en grensveranderingen in het openbaar bestuur*, Alphen aan den Rijn: Samsom.

Bekkers, V.J.J.M. & S. Zouridis (1999) 'Electronic service delivery in public administration: Some trends and issues', *International Review of Administrative Sciences* 65: 183-195.

Bekkers, V.J.J.M. (2000) *Voorbij de virtuele organisatie? Over de bestuurskundige betekenis van virtuele variëteit, contingentie en parallel organiseren*, Den Haag: Elsevier.

Bekkers, V.J.J.M. (2001) 'De mythen van de elektronische overheid. Over retoriek en realiteit', *Bestuurswetenschappen* 4: 277-295.

Bekkers, V.J.J.M. & M. Thaens (2002) 'E-government op een kruispunt van wegen', *Bestuurskunde* 8: 328-337.

Bekkers, V., M. Lips & A. Zuurmond (2005) 'De januskop van ICT in het publieke domein', blz. 733-752 in M. Lips et al. (red.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma.

Bekkers, V. & M. Thaens (2005) 'Sturing, informatie en ICT', blz. 137-160 in M. Lips et al. (red.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma.

Bekkers, V., H. van Duivenboden & M. Lips (2005) 'ICT en publieke dienstverlening', blz. 237-256 in M. Lips et al. (red.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid,* Utrecht: Lemma.

Bekkers, V.J.J.M. & V. Homburg (2009) 'The myths and ceremonies of E-Government: beyond the hype of a new and better government?', blz. 217-234 in A. Meijer et al. (red.) *ICTs, citizens and governance: after the hype*, Amsterdam: IOS Press.

Bekkers, V.J.J.M. & A. Meijer (2010) *Cocreatie in de publieke sector. Een verkennend onderzoek naar nieuwe, digitale verbindingen tussen overhead en burger*, Den Haag: Boom Juridische Uitgevers.

Bemt, P. van den (2006) HARM *(Hospital Admissions Related to Medication*), Utrecht: Universiteit van Utrecht.

Bennett, C. J. (2008) *The privacy advocates: Resisting the spread of surveillance,* Cambridge MA: MIT Press 2008.

Berg, B. van den (2008) 'Ik doe er niet aan mee. Niet-gebruikers in een technologische wereld', blz. 263-280 in M. van den Berg, C. Prins & M. Ham (red.) *In de greep van de technologie. Nieuwe toepassingen en het gedrag van de burger*, Amsterdam: Van Gennep.

Berg, M. van den, C. Prins & M. Ham (2008) *In de greep van de technologie. Nieuwe toepassingen en het gedrag van de burger*, Amsterdam: Van Gennep.

Berg, B. van den (2009) 'Slijp de messen', *Flux september 2009*, Rathenau Instituut: Den Haag.

Berg, B. van den & R.E. Leenes (2011) 'Keeping up appearances: Audience segregation in social network sites' in P. de Hert (red.) *Computers, privacy and data protection: An element of choice,* Springer 2011, forthcoming.

Berkvens, J.A. (1992) 'Van Heerendiensten naar Informatiediensten', blz. 109-130 in P.H.A. Frissen et al. (red.) *Orwell of Athene Democratie en Informatiesamenleving,* Den Haag: Sdu.

Besters, Michiel (2010) 'De schaduwzijden van het Schengen Informatie Systeem', blz. 74-85 in Geert Munnichs et al. (red.) *Databases. Over ICT-beloftes, informatiehonger en digitale autonomie*, Den Haag: Rathenau Instituut.

Besters, Michiel & Frans Brom (2010) 'Greedy information technology: The digitalization of the European migration policy', *European Journal of Migration and Law* 12: 455-470.

Bijker, W. & J. Law (red.) (1992) *Shaping technology/Building society. Studies in sociotechnical change,* Cambridge, MA: MIT Press.

Bijker, W. (2001) 'Understanding technological culture through a constructivist view of science, technology, and society', blz. 19-34 in S. Cutcliffe & C. Mitcham (red.) *Visions of STS: Counterpoints in science, technology, and society studies*, New York: State University of New York Press.

Biometric Technology Today (2009) 'Biometrics review: 2008/2009', *Biometric Technology Today,* January 2009: 9-11.

Blok, P. (2002) *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Den Haag: Boom Juridische Uitgevers.

Boersma, K., A. Meijer & P. Wagenaar (2009) 'Unraveling and understanding the e-government hype', blz. 217-234 in A. Meijer et al. (red.) *ICTs, Citizens and governance: after the hype*, Amsterdam: IOS Press.

Böhre, V. (2010) *Happy landings? Het biometrische paspoort als zwarte doos*, WRR-webpublicatie nr. 46, www.wrr.nl.

Borking, J.J.F.M. (2010) *Privacyrecht is Code, Over het gebruik van privacy enhancing technologies*, dissertatie, Leiden.

Borst, W.L. (2009) *Jegens en Wegens. Over persoonsgebonden informatie in de strafrechtsketen*, Nijmegen: Wolf Legal Publishers.

Boschker, E., P. Castenmiller & A. Zuurmond (2010) 'Dynamiek in de gemeentelijke basisadministratie', blz. 86-98 in Geert Munnichs et al. (red.) *Databases. Over ICT-beloftes, informatiehonger en digitale autonomie*, Den Haag: Rathenau Instituut.

Boswell, C. (2007) 'Migration control in Europe after 9/11: explaining the absence of securitization', *Journal of Common Market Studies* 45, 3: 589-610.

Boutellier, H. (2003) De *veiligheidsutopie: Hedendaags onbehagen en verlangen rond misdaad en straf.* Den Haag: Boom Juridische Uitgevers.

Boutellier, J.C.J. (2007) *Nodale orde: Veiligheid en burgerschap in een Netwerksamenleving*, Oratie Vrije Universiteit, Amsterdam.

Bovens, M. & S. Zouridis (2002) 'From street-level tot system-level bureaucracies: How information and communication technology is transforming administrative discretion and constitutional control', *Public Administration Review* 62, 2: 174-184.

Bovens, M. (2003) *De digitale republiek. Democratie en rechtsstaat in de informatiemaatschappij*, Amsterdam: Amsterdam University Press.

Boyd, D. (2008) *Taken out of context: American teen sociality in networked publics*, PhD Dissertation, University of California-Berkeley, School of Information.

Broeders, D. (2007) 'The new digital borders of Europe. EU databases and the surveillance of irregular migrants', *International Sociology* 22, 1: 71-92.

Broeders, D. (2009) *Breaking down anonymity. Digital surveillance of irregular migrants in Germany and the Netherlands.* Amsterdam: Amsterdam University Press.

Broeders, D. (2011) 'Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa' in D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.) *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press.

Broeders, D., C.M.K.C. Cuijpers & J.E.J. Prins (red.) (2011) *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press.

Brouwer, E. (2008) *Digital borders and real rights. Effective remedies for third-country nationals in the Schengen information system*, Leiden/Boston: Martinus Nijhoff Publishers.

Burger@Overheid.nl (2006) *Werkschrift BurgerServiceCode*, Versie 2.2 http://www.burger.overheid.nl/files/bsc_schrift_versie_2.2._december_2006_.pdf, geraadpleegd op 22 november 2010.

Burger@Overheid.nl (2007) *Het geweten van de elektronische overheid. Vijf jaar Burger@Overheid.nl (2002-2007)*, Den Haag.

Buruma, Y. (2011) 'Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld', in D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.) *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press.

Canhoto, A. & J. Backhouse (2008) 'General description of the process of behavioral profiling', blz. 47-64 in M. Hildebrandt & S. Gutwirth (red.) *Profiling the European citizen. Cross-disciplinary perspectives,* België/Nederland: Springer.

CapGemini Consulting & Ernst & Young (2004) *De koers van de keten. Een verkennend onderzoek naar de consequenties van digitalisering in de bestemmingsplanketen*, Onderzoek in opdracht van de Provincie Noord-Brabant en Ministerie van VROM, Utrecht.

CapGemini Consulting (2010a) *eRijbewijs. CapGemini onderzoek naar het eRijbewijs en haar relatie met andere initiatieven*, Utrecht.

CapGemini Consulting (2010b), *Interoperabiliteit binnen en tussen sectoren,* Verkenning voor het Forum Standaardisatie naar e-dossiers, verwijsindexen en registers, Den Haag.

Caplan, J. & J. Torpey (2001) 'Introduction' blz. 1-12 in J. Caplan & J. Torpey (red.) *Documenting individual identity. The development of state practices in the modern world,* Princeton: Princeton University Press.

Castells, M. (1996, second edition 2000) *The rise of the network society, The information age: Economy, society and culture I*, Cambridge MA: Blackwell.

Centraal Bureau voor de Statistiek (2009a) *De digitale economie*, Den Haag.

Centraal Bureau voor de Statistiek (2009b) *Integrale Veiligheidsmonitor 2008*, http://www.cbs.nl/NR/rdonlyres/DD316B79-27F4-4370-A0D4-BE0514248B4B/0/2008integraleveiligheidsmonitorlandelijk.pdf.

Centraal Informatiepunt Onderzoek Telecommunicatie (2010a) *Jaarverslag 2009*, Den Haag.

Centraal Informatiepunt Onderzoek Telecommunicatie (2010b) *Eindrapport Audit CIOT en omgevingen 2009*, Den Haag 19 april 2010.

Centraal Planbureau (2004) *Zelfevaluatie door het College bescherming persoonsgegevens (CBP) van het toezicht op de verwerking van persoonsgegevens*, Den Haag, 30 maart 2004.

Chandler, D. (1996) 'Engagement with media: shaping and being shaped', *Computer-Mediated Communication Magazine,* beschikbaar via http://www.december.com/cmc.

Chavannes, M. (2009) *Niemand regeert. De privatisering van de Nederlandse politiek*, Rotterdam: NRC Boeken.

Choenni, S., E. Leertouwer & T. Busker (2011) 'Klachten over toepassingen van informatietechnologie. Analyse van een aantal overheidsbestanden' in D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.) *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press.

Clarke, R. (1988) 'Information Technology and Dataveillance', *Communications of the ACM* 31, 5: 498-512.

Clarke, R. (1994) 'The digital persona and its application to data surveillance', *The Information Society,* 10,2, http://www.rogerclarke.com/DV/DigPersona.html, geraadpleegd op 23 augustus 2010.

College Bescherming Persoonsgegevens (2006) *Notitie Fraudebestrijding door bestandskoppeling*, Den Haag, september 2006.

College Bescherming Persoonsgegevens (2007) Advies Wetsvoorstel implementatie bewaarplicht, 22 januari 2007.

College Bescherming Persoonsgegevens (2008) *Jaarverslag 2007,* Den Haag.

College Bescherming Persoonsgegevens (2009) *Jaarverslag 2008*, Den Haag.

College Bescherming Persoonsgegevens (2010a) *Onderzoek naar de verwerking van het burgerservicenummer en kopie identiteitsbewijs voor de Rijkspas door de minister*

van Verkeer en Waterstaat, z2010-00050, 27 mei 2010. Zie http://www.cbpweb.nl/Pages/med_20100607_rijkspas.aspx.

College Bescherming Persoonsgegevens (2010b) *Rapport over bestandskoppelingen door de SIOD voor de ontwikkeling van risicoprofielen*, Den Haag, mei 2010.

College Bescherming Persoonsgegevens (2010c) *Jaarverslag 2009*, Den Haag.

College en Forum Standaardisatie (2009) *Jaarverslag 2009*, Den Haag, 23 februari 2010.

Commissie-Brouwer-Korf (2009) *Gewoon Doen. Beschermen van veiligheid en persoonlijke levenssfeer*, Rapport aan de ministers van Justitie en Binnenlandse Zaken, Den Haag.

Commissie-Jorritsma (2005) *Publieke dienstverlening, professionele gemeenten. Visie 2015*, Den Haag: VNG.

Commissie-Mevis (2001) *Rapport van de Commissie Strafvordelijke gegevensvergaring in de informatiemaatschappij*. Kamerstukken II, 2001/02, 28366, nr. 1.

Commissie-Postma-Wallage (2007) *Het uur van de waarheid*, Den Haag.

Commissie-Suyver (2009) *Naar een integrale evaluatie van antiterrorismemaatregelen*, Rapport van de Commissie evaluatie antiterrorismebeleid, Den Haag.

Cuijpers, C.M.K.C. & E.J. Koops (2009) 'Begluren en besturen door slimme energiemeters: een ongerechtvaardigde inbreuk op onze privacy', *Privacy en Informatie* 1: 2-8.

Cukier, K. (2010) *Metadata Matters. META: The rise and governance of information about information. A report of the 2010 global leaders of information policy conference*, Singapore.

Custers, B. (2004) *The power of knowledge. Ethical, legal, and technological aspects of data mining and group profiling in epidemiology*, Nijmegen: Wolf Legal Publishers.

Deleuze, G. (2002) 'Postscript on control societies', blz. 316-321 in T. Levin, U. Frohne & P. Weibel (red.) *CTRL [SPACE]. Rhetorics of surveillance from Bentham to Big Brother*, Cambridge, MA: MIT Press.

Deursen, A.J.A.M. van, J.A.G.M. van Dijk & D. Boland (2007) *Elektronische publieke dienstverlening in de toekomst. Opinies over de strategische doelstellingen en perspectieven achter elektronische overheidsdienstverlening*, Onderzoeksrapport Universiteit Twente.

Deursen, A.J.A.M. van & J.A.G.M. van Dijk (2010) *Trendrapport Computer- en Internet-gebruik 2010. Een Nederlands en Europees perspectief*, Enschede: Universiteit Twente.

Dijk, van J. (2007) 'De e-surfende burger: is de digitale kloof gedicht?', blz. 31-50 in J. Steyaert & J. de Haan (red.) *Jaarboek ICT en samenleving. Gewoon digitaal,* Amsterdam: Boom.

Dijstelbloem, H. & A. Meijer (2009) *De Migratiemachine. De rol van technologie in het Migratiebeleid*, Amsterdam: Van Gennep.

Dijstelbloem, H. & J.W. Holtslag (2010) 'De veranderende architectuur van het bestuur', blz. 15-54 in H. Dijstelbloem, P. den Hoed, J.W. Holtslag & S. Schouten (red.) *Het gezicht van de publieke zaak. Openbaar bestuur onder ogen*, WRR-verkenning 23, Amsterdam: Amsterdam University Press.

Donk, W. van de, & P. Depla (1993) 'Wie stuurt de vernieuwing? Raadsinformatiesystemen als ontmoeting van politiek en technologie', *Bestuurskund*e 2, 6.

Donk, W.B.H.J. van de, & O. Meyer (1994) 'Beleid voor informatisering', blz. 29-68 in A. Zuurmond et al. *Informatisering in het openbaar bestuur. Technologie en sturing bestuurskundig beschouwd,* Den Haag: VUGA.

Donk, W.B.H.J. van de & P.H.A. Frissen (1994) 'Informatisering, Wetgeving en Sturing', blz. 35-64 in Ph. Eijlander et al. (red.) *Wetgeven en de maat van de tijd* (red.), Zwolle: Tjeenk Willink.

Donk, W.B.H.J. van de (1997) *De arena in schema. Een verkenning van de betekenis van informatisering voor beleid en politiek inzake de verdeling van middelen onder verzorgingshuizen*, dissertatie, Tilburg.

Donk, W.B.H.J. van de & R. van Dael (2005) 'Overheid en ICT: Kroniek van een beleid', blz. 161-196 in M. Lips et al. (red.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma.

Ducastel, N. (2008) 'Europese interoperabiliteit: langzaam en zeker?!', blz. 283-293 in S. Zwienink & P. Wisse. (red.) *Eerlijk zullen we alles delen. Verkenningen naar interoperabiliteit*, GBO.Overheid/Bureau Forum Standaardisatie, Den Haag.

Duivenboden, H.P.M. van (1999) *Koppeling in uitvoering. Een verkennende studie naar de betekenis van het koppelen van persoonsgegevens door uitvoerende overheidsorganisaties voor de positie van de burger als cliënt van de overheid*, Delft: Eburon.

Duivenboden, H.P.M. van et al. (red.) (2000) *Ketenmanagement in de publieke sector*, Utrecht: Lemma.

Duivenboden, H.P.M. van & M. Rietdijk (2005) *Puzzelen met Prioriteit. Een strategische verkenning van het absorptievermogen van gemeenten met betrekking tot de implementatie van ICT-vernieuwingen.* Onderzoek in opdracht van ministerie van BZK en het VNG, CapGemini: Utrecht.

Dunleavy, P., H. Margetts, S. Bastow & J. Tinker (2006) *Digital era governance: IT corporations, the State, and e-government*, Oxford: Oxford University Press.

Dutton, W.H. (1999) *Society on the line. Information politics in the digital a*ge, Oxford: Oxford University Press.

Dworkin, R. (1977) *Taking rights seriously*, Cambridge, MA: Harvard University Press.

eCall Driving Group (2005) *eCall Driving Group: Participants*, http://www. esafety support.org/en/ecall_toolbox/index.html, geraadpleegd op 3 november 2010.

ECP-EPN (2010) *Van beschikbaarheid naar toepassing. Aanbevelingen gericht op concurrentiekracht, de energievoorziening, de zorg, de mobiliteit, de overheidsdienstverlening en het onderwijs*, Leidschendam.

Edge, D. (1995) 'The social shaping of technology', blz. 14-32 in N. Heap, R. Thomas, G. Einon, R. Mason & H. Mackay (red.) *Information, technology and society,* London: Sage.

EDPS (2006) *Opinion of the European data protection supervisor*, Brussels, 20 January 2006.

Edwards, G. & C.O. Meyer (2008) 'Introduction: Charting a contested transformation' in *JCMS* 46, 1: 1-26.

Eenmalige Adviescommissie ICT en Overheid (2001) *Burger en overheid in de informatiesamenleving. De Noodzaak van institutionele innovatie*, Den Haag.

Eerste Kamer (2006-2007) *Behandeling wetsvoorstel BSN*, Kamerstukken I, 30312, B.
Eerste Kamer (2007-2008) *Brief Vaste Commissie voor Binnenlandse Zaken over de notitie burgerservicenummer*, Kamerstukken I, 30312, J.
Eerste Kamer (2008-2009a) *Behandeling wetsvoorstel slimme energiemeters*, Handelingen I, nr. 26.
Eerste Kamer (2008-2009b) *Behandeling herinrichten reisdocumentenadministratie*, Handelingen I, nr. 34, blz. 1563 e.v.
Eerste Kamer (2009-2010a) *Verslag Schriftelijk Overleg inzake evaluatie WBP,* Kamerstukken I, 31051, A.
Eerste Kamer (2009-2010b) *Verslag van een rondetafel over het EPD*, Kamerstukken I, 31466, nr. K.
Eerste Kamer (2009-2010c) *Memorie van antwoord – Wijziging van de Wet gebruik burgerservicenummer in de zorg*, Kamerstukken I, 31466, C.
Eerste Kamer (2009-2010d) *Voorlopig verslag van overleg over Wijziging van de Wegenverkeerswet 1994*, Kamerstukken I, 31896, nr. B.
Eerste Kamer (2009-2010e) *Memorie van Antwoord – Wijziging van de Wegenverkeerswet 1994*, Kamerstukken I, 31896, nr. C.
Eerste Kamer (2009-2010f) *Brief staatssecretaris betreffende de toekenning, het beheer en het gebruik van het Burgerservicenummer*, Kamerstukken I, 30312, nr. L.
Eerste Kamer (2010-2011) *Korte aantekeningen vergadering van de vaste commissies van BZK, de JBZ-Raad, Justitie, OC&W en VWS*, 7 december 2010, http://www.eerstekamer.nl/behandeling/20101207/korte_aantekening_9/ f=/vikzc6ylr2ho.pdf, geraadpleegd op 4 januari 2011.
Eeten, M. van (2010) *Techniek van de onmacht: Fatalisme in politiek en technologie*, oratie Delft.
Eeten, M. van (2011) 'Gedijen bij onveiligheid. Afwegingen rond de risico's van informatietechnologie' in D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.) *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press.
Eijkman, Q. (2010) 'Liever geen bekende Nederlander zijn. Het mobiliseren van mensenrechten en de bescherming van digitale persoonsgegevens', blz. 65-72 in *16 miljoen BN'ers? Bescherming van persoonsgegevens in het Digitale Tijdperk 47*, Leiden: Stichting NJCM-Boekerij.
Ellul, J. (1954) *La technique ou l'enjeu du siecle*, Paris: Armand Collin.
Ellul, J. (1977) *La systeme technicien*, Paris: Calmann-Levy.
Est, R. van, C. van 't Hof, D. van Harten (red.) (2007) *RFID: meer keuze, gemak en controle in de digitale publieke ruimte,* Den Haag: Rathenau Instituut.
Europese Commissie (1999) *Europe: een informatiemaatschappij voor iedereen*, COM (1999) 687 def.
Europese Commissie (2001) *European governance, a white paper*, Brussel, http://eur-ex.europa.eu/LexUriServ/site/en/com/2001/com2001_0428en01.pdf, geraadpleegd op 16 november 2009.
Europese Commissie (2002) *Actieplan eEurope 2005: Een informatiemaatschappij voor iedereen,* COM (2002) 263 def.

Europese Commissie (2003) *Ontwikkeling van het Schengeninformatiesysteem II en mogelijke synergie met een toekomstig visuminformatiesysteem (VIS)*, COM (2003) 771 def.
European Commission (2005) *A fine balance: Privacy enhancing technologies: How to create a trusted information society – summary of conference*, Brussels.
Europese Commissie (2010a) *Mededeling inhoudende Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht*, COM (2010) 385 def.
Europese Commissie (2010b) *Mededeling inzake doorgifte van passagiersgegevens (PNR)*, COM (2010) 492 def.
Europese Commissie (2010c) *Europese Commissie presenteert strategie voor versterking gegevensbeschermingsregels EU*, IP/10/1462.
Expertcommissie informatievoorziening en elektronische dienstverlening SUWI (2005) *De Burger Bediend*, Den Haag.
Facebook (2010) Perskamer, http://www.facebook.com/press/info.php?statistics, geraadpleegd op 27 september 2010.
Februari, Marjolein (2008) 'Variaties op de standaard', Den Haag: Forum Standaardisatie 2008, blz. 91-92.
Ferwerda, H., E. van der Torre & V. van Bolhuis (2010) *Nodale praktijken. Empirisch onderzoek naar het nodale politieconcept, Politie en Wetenschap*, Bureau Beke, COT Instituut voor Veiligheid en Crisismanagement, Apeldoorn, Arnhem, Den Haag.
Fijnaut, C. (2007) 'De ontwikkeling van de politiële samenwerking in de Europese Unie: verworvenheden en uitdagingen', blz. 109-138 in J. Meeusen & G. Straetmans (red.) *Politiële en justitiële strafrechtelijke samenwerking in de Europese Unie. Welk evenwicht tussen vrijheid, veiligheid en rechtvaardigheid?*, Antwerpen: Intersentia.
Fleck, J. (1993) 'Configurations: Crystallizing contingency', *International Journal on Human Factors in Manufacturing* 3: 15-36.
Floridi, L. (2005) 'The ontological interpretation of information privacy', *Ethics and Information Technology:* 185-200.
Florini, A. (1998) 'The end of secrecy', *Foreign Policy,* blz. 50-63.
Forum Standaardisatie (2010) *Sturen op Open Standaarden. Een handreiking voor overheidsorganisaties*, Den Haag.
Foucault, M. (1977) *Discipline and punish. The birth of the prison*, New York: Vintage.
Fountain, J. (2001) 'Paradoxes of public sector customer service', *Governance: An international journal of policy and administration* 14, 1: 55-73.
Franken, H. (1993) 'Kanttekeningen bij het automatiseren van beschikkingen' in *Beschikken en Automatiseren. Preadvies voor de Vereniging voor Bestuursrecht*, VAR-reeks nr. 110, Den Haag.
Fredman, S. (2008) *Human rights transformed: Positive rights and positive duties*, Oxford: Oxford University Press.
Frissen, P.H.A. (1989) *Bureaucratische cultuur en informatisering. Een studie naar de betekenis van informatisering voor de cultuur van een overheidsorganisatie*, Den Haag: Sdu Uitgeverij.
Frissen, P.H.A. (1996) *De virtuele staat. Politiek, bestuur, technologie: een postmodern verhaal*, Schoonhoven: Academic Service.

Frissen, V. (2004) *De Domesticatie van de Digitale Wereld*, rede uitgesproken bij de aanvaarding van het ambt van bijzonder hoogleraar 'ICT en Sociale Verandering' vanwege het LIFT-fonds van TNO aan de Faculteit der Wijsbegeerte van de Erasmus Universiteit Rotterdam. http://www.publiek-politiek.nl/Bestanden/the-XPIN-files/De-domesticatie-van-de-digitale-wereld-Valerie-Frissen, geraadpleegd op 23 augustus 2010.

Frissen, V.M. (2008) 'Digitaal knutselen. De doorbraak van het wilde denken', blz. 15-27 in V.M. Frissen & J. de Mul (red.) *De draagbare lichtheid van het bestaan*, Kampen: Klement/Pelckmans.

Frissen, P.H.A. (2009) *Gevaar verplicht. Over de noodzaak van aristocratische politiek*, Amsterdam: Van Gennep.

Fuglsang, L. (2001) 'Three perspectives in STS in the policy Context', blz. 35-50 in S. Cutcliffe & C. Mitcham (red.) *Visions of STS. Cointerpoints in science, technology, and society studies,* New York: State University of New York Press.

Fung, A., M. Graham & D. Weil (2007) *Full disclosure: the perils and promise of transparency*, Cambridge: Cambridge University Press.

Garland, D. (2001) *The culture of control*, Oxford: Oxford University Press.

Gateway NUP (2009) *Wederzijdse gijzeling in machteloosheid, of de As van het Goede?,* Rapportage NUP-review.

George, A. & A. Bennet (2004) *Case studies and theory development in the social sciences*, Cambridge, MA: MIT Press.

Gilder, G. (1994) *Life after television: The coming transformation of media and American life*, New York: W.W. Norton.

Gilliom, J. (2001) *Overseers of the poor. Surveillance, resistance, and the limits of privacy,* Chicago: University of Chicago Press.

Gómez-Arostegui, H.T. (2005) 'Defining private life under the European convention on human rights by referring to reasonable expectations', *California Western International Law Journal* 35: 153-202.

Gomez-Barrosso, J.L., C. Feijoo & E. Karnitis (2008) 'The European policy for the development of an information society: The right path?', *Journal of Common Market Studies* 46, 4: 787-825.

Govcert.nl (2009) *Trendrapport 2009. Inzicht in cybercrime: trends en cijfers*, Den Haag: Ministerie van BZK.

Govcert.nl (2010) *Jaarverslag 2009*, Den Haag.

Gribnau, J.L.M. (2010) 'Kenbare fouten en navordering. Grondslagen in het licht van automatisering en mensen', *Weekblad Fiscaal Recht*, 2010/214.

Griffioen, H. (2011) *'Location based privacy' in constellaties van publiek-private verantwoordelijkheid*, WRR-webpublicatie nr. 59, te verschijnen.

Grijpink, J.H.A.M. (2006a) *Keteninformatisering in kort bestek: theorie en praktijk van grootschalige informatie-uitwisseling*, Den Haag: Lemma.

Grijpink, J.H.A.M. (2006b) 'Identiteitsfraude en overheid', *Justitiële Verkenningen* 32, 7: 36-56.

Groot, H. de (2010) *Evidence-based public management*, oratie Universiteit Twente, 3 juni 2010.

Groothuis, M.M. (2010) 'De Awb en digitalisering', blz. 343-358 in T. Barkhuysen et al. (red.) *Bestuursrecht harmoniseren: 15 jaar Awb*, Den Haag: Boom Juridische Uitgevers.

Guild, E. (2009) *Security and migration in the 21st century*, Cambridge: Polity Press.

Gunsteren, H. van (2004) *Gevaarlijk Veilig. Terreurbestrijding in de democratie*, Amsterdam: Van Gennep.

Gunsteren, H. van (2006) *Vertrouwen in de democratie. Over principes van zelforganisatie*, Amsterdam: Van Gennep.

Gunsteren, H. van (2009) 'Burgerschap in Nederland 1992-2008: voortschrijdend inzicht?', *B en M* 36, 1: 41-49.

Haan, J. de (2004) 'ICT en samenleving', blz. 223-264 in *In het zicht van de toekomst, sociaal en cultureel rapport 2004*, Den Haag: Sociaal en Cultureel Planbureau.

Haan, J. de & L. van der Laan (2005) *Jaarboek ICT en samenleving. Kennis in netwerken*, Amsterdam: Boom.

Haggerty, K. & R. Ericson (2000) 'The surveillant assemblage', *British Journal of Sociology* 51, 4: 605-622.

Hampshire, J. & D. Broeders (2010) *The digitalization of European borders and migration controls*, Pilot study for the Migration to Europe in the Digital Age (MEDiA) project, http://www.mediaresearchproject.eu/reports/Report2_Borders.pdf, geraadpleegd op 11 november 2010.

Haratsch, A. (2006) 'Allgemeine Handlungsfreiheit', blz. 558-572 in F.S.M. Heselhaus & C. Nowak (Hrsg.) *Handbuch der Europäischen Grundrechte*, München: Beck.

Harcourt, B.E. (2007) *Against prediction: profiling, policing, and punishing in an actuarial age*, Chicago: University of Chicago Press.

Hayes, B. (2009) *NeoConOpticon. The EU security-industrial complex.* Amsterdam/London: Transnational Institute/Statewatch.

HEC (2007) *Naar een goed gebruik van het burgerservicenummer (BSN)*, Papernote nr. 21, P. Heemskerk et al., Den Haag.

Hermans, K. (2010) 'Het gebruik van vingerafdrukken voor opsporingsdoeleinden onder de nieuwe paspoortwet en artikel 8 EVRM', *Nederlands Tijdschrift voor de Mensenrechten/NJCM Bulletin* 1: 35-40.

Hert, P. de & B. de Schutter (2008) 'International transfers of data in the field of JHA: The lessons of Europol, PNR and Swift', blz. 299-335 in B. Martenczuk & S. van Thiel (red.) *Justice, Liberty, Security: New challenges for EU external relations*. Brussels: VUB Press.

Hert, P. de (2009) *In het licht van de technologie. Pleidooi voor continuïteit en verandering bij gegevensbescherming*, College Bescherming Persoonsgegevens, Den Haag.

Hert, P. de (2011) 'Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechten verplichting' in D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.) *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press.

Hildebrandt, M. & S. Gutwirth (red.) (2008) *Profiling the European citizen. Cross-disciplinary perspectives,* Belgium/Netherlands: Springer.

Hildebrandt, M. (2008) 'Defining profiling: A new type of knowledge', blz. 17-45 in

M. Hildebrandt & S. Gutwirth (red.) *Profiling the European citizen. Cross-disciplinary perspectives,* Belgium/Netherlands: Springer.

Hirsch Ballin, E.M.H. (1986) 'De legitimiteit van de selectie van informatie', *Ars Aequi* 35, 11: 726-730.

Hirsch Ballin, E.M.H. (1992) 'Democratie en informatiesamenleving', blz. 77-85 in P.H.A. Frissen et al. (red.) *Orwell of Athene. Democratie en informatiesamenleving*, Den Haag: Sdu.

Hirsch Ballin, E.M.H. (1993) 'De gekoppelde staat', blz. 61-74 in L.A. Geelhoed et al. (red.) *Wetgeving in Beweging,* Zwolle: Tjeenk Willink.

Hobbing, P. & R. Koslowski (2009) *The tools called to support the 'delivery' of freedom, security and justice: A comparison of border security system in the EU and in the US*, Ad Hoc Briefing Paper, European Parliament, Directorate-General Internal Policies, Policy Department C, Citizens' Rights and Constitutional Affairs, Committee on Civil Liberties, Justice and Home Affairs, PE 410.681.

Hof, S. van der, R. Leenes & S. Fennell (2009) *Framing citizen's identities. The construction of personal identities in new modes of government in the Netherland*s, Tilburg.

Hof, S. van der & E. Keymolen (2010) 'Shaping minors with major shifts: Electronic child records in the Netherlands', *Information Polity,* 15, 4: 309-322.

Hof, C. van 't, R. van Est & F. Daemen (2010) *Check in/Check out. De digitalisering van de openbare ruimte.* Den Haag: Rathenau Instituut.

Holla, Poelman & Van Leeuwen advocaten (2008), *brief*, 28 maart 2008.

Holvast, J. & M.J. Bonthuis (2010) *Blackbox-onderzoek Veiligheidshuizen*, WRR-webpublicatie nr. 49, www.wrr.nl.

Hoogwout, M. (2010) *De rationaliteit van de klantgerichte overheid. Een onderzoek naar de spanningen die de invoering van het klantdenken bij gemeenten veroorzaakt en de manier waarop gemeenten daarmee omgaan*, Nieuwegein: Uitgeverij Réunion.

Horrocks, I. (2009) 'Experts' and e-Government. Power, influence and the capture of a policy domain in the UK', *Information, Communication en Society* 12, 1: 110-127.

Horsley, J. (2007) 'Towards a More Open China?', blz. 54-91 in A. Florini (red.) *The right to know*, Chichester: Columbia University Press.

House of Commons Home Affairs Committee (2008) *A surveillance society?*, Fifth Report of Session 2007-08 (2 Volumes), London: Stationery Office.

House of Lords (2007) Schengen Information System (II) (SIS II), Report with evidence, 9th Report of Session 2006-7 of the House of Lords' European Union Committee, Londen: The Stationary Office Limited.

House of Lords (2009) Surveillance: Citizens and the State, Londen: 6 februari 2009.

Hout, E. van (2005) 'Kosten en baten van ICT en informatievoorziening in het openbaar bestuur', blz. 257-276 in M. Lips et al. (red.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma.

Hoven, J. van den (1998) 'Moral responsibility, public office and information technology', blz. 97-106 in I. Snellen & W. van de Donk (red.) *Public administration in an information age. A handbook*, Amsterdam: IOS Press.

Hughes, T. (1994) 'Technological Momentum', blz. 101-115 in M. Smith & L. Marx (red.) *Does technology drive history? The dilemma of technological determinism,* Cambridge, MA: MIT Press.

Hurenkamp, M. & M. Kremer (red.) (2005) *Vrijheid Verplicht. Over tevredenheid en de grenzen van keuzevrijheid*, Amsterdam: Van Gennip.

Huydecoper, S., G. Lekkerkerker & P. van Schelven (2001) 'Van e-overheid en wijze mannen', blz. 57-72 in P. van Schelven et al. (red.) *@-Government. Virtuele fictie of blijvend toekomstbeeld?, Nederlandse Vereniging voor Informatietechnologie en Recht, preadviezen 2001,* Den Haag: Elsevier.

Hyves (2010) http://www.hyves.nl, geraadpleegd op 16 juni 2010.

Infodrome (2001) *Controle geven of nemen. Een politieke agenda voor de informatiesamenleving*, Amsterdam: Otto Cramwinckel.

Informatie Beheer Groep (2009) *Jaarverslag 2008*, Groningen.

Information Commissioner's Office (2007) *Data protection strategy consultation*, Draft.

Johnson, D.G. & J.M. Wetmore (red.) (2009) *Technology and society. Building our sociotechnical future*, Cambridge, MA: MIT Press.

Johnston, L. & C. Shearing (2003) *Governing security. Explorations in policing and justice*, London: Routledge

Jurgens, E. (2005) 'NJCM: ontdek het parlement! Een aansporing aan het NJCM om het parlement te helpen bij zijn kritiek op verdragen en EU-besluiten in voorbereiding', *Terrorismebestrijding met mensenrechten*, Leiden: NJCM-Boekerij nr. 42.

Kaplan, D. (2009) *Readings in the philosophy of technology,* 2nd ed., Lanham, MD: Rowman & Littlefield.

Kearns, I. (2004) *Public value and e-government*, London: Institute for Public Policy Research (IPPR).

Keizer, A.G. (2011) 'De digitale patiënt centraal. Medische informatie in een digitale wereld' in D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.) *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press.

Keymolen, E. (2007) *Onzichtbare zichtbaarheid. Plessner ontmoet profiling* (scriptie EUR).

Keymolen, E.L.O. & D. Broeders (2010) 'Verloren onschuld. Inzicht en toezicht binnen de Verwijsindex Risicojongeren', blz. 73-89 in W. Pieters et al. (red.) *Inzicht en toezicht. Controle in de Kennissamenleving*, Jaarboek Kennissamenleving 2010, Amsterdam: Aksant.

Keymolen, E., J.E.J. Prins & C. Raab (2011) 'Trust and ICT: New challenges for public administration' in I.Th.M. Snellen, M. Thaens, W.B.H.J. van de Donk (red.) *Public administration in an information age*, IOS Press, te verschijnen.

Keymolen, E.L.O. en J.E.J. Prins (2011) 'Jeugdzorg via systemen. De verwijsindex risicojongeren als spin in een digitaal vangnet' in D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.) *De staat van informatie,* WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press.

Kielman, H. (2010) *Politiële gegevensverwerking en privacy*, dissertatie, Leiden.

Kinkhorst, O. (2000) 'Het RINIS-concept: keteninformatisering in de sociale zekerheid',

blz.175-184 in H. van Duivenboden et al. (red.) *Ketenmanagement in de publieke sector,* Utrecht: Lemma.
Klein, E. (2003) 'Why should a computer be anything like a human being?', *I3 Magazine*: blz. 30-32. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.8768 enrep=rep1entype=pdf, geraadpleegd op 17 augustus 2010.
Knaap, P. van der (2010) 'Veiligheidsbeleid: onderbouwd en effectief? De meerwaarde van beleidstheorieën voor beleid en beleidsevaluatie' *Tijdschrift voor veiligheid* 9, 1: 6-21.
Kohnstamm, J. & L. Dubbeld (2007) 'Glazen samenleving in zicht', *Nederlands Juristenblad* 37: 2369-2375.
Kok, W. de, R. Scholtbach & J. van der Vleuten (2001) 'De onzichtbare hand van de overheid. Over de rol van de overheid en de functie van ICT', blz. 281-302 in H. van Duivenboden & M. Lips (red.) *Klantgericht werken in de publieke sector. Inrichting van de elektronische overheid*, Utrecht: Lemma.
Koops, B.J. (2006) *Tendensen in opsporing en technologie: Over twee honden en een kalf*, Oratie, Tilburg.
Koslowski, R. (2008) 'Global mobility and the quest for an international migration regime', blz. 103-143 in J. Chamie & L. Dall'Oglio (red.) *International migration and development: Continuing the dialogue: Legal and policy perspectives*, Geneva: International Organization for Migration.
Kroes, N. (2010) Memo 10/33, date 09/02/2010, te raadplegen op www.europa.eu/rapid/searchAction.do.
Kroon, N. & V. Bekkers (1994) 'Informatiesystemen in Europa: een slagader of een slagveld', blz. 69-82 in A. Zuurmond et al. (red.) *Informatisering in het openbaar bestuur. Technologie en sturing bestuurskundig beschouwd,* Den Haag: VUGA.
Kumar, K. (2004) 'Bringing it all back home. A comment on Iris Young', blz. 187-193 in B. Rössler (red.) *Privacies. Philosophical evaluations*, Stanford: Stanford University Press.
Laan, L. van der & J. de Haan (2005) 'ICT in de kennis –en netwerkeconomie', blz. 13-32 in J. de Haan et al. (red.) *Jaarboek ICT en samenleving. Kennis in netwerken*, Amsterdam: Boom.
Lahav, G. & V. Guiraudon (2000) 'Comparative perspectives on border control: Away from the border and outside the state', blz.55-77 in P. Andreas & T. Snyder (red.) *The wall around the West. State borders and immigration controls in North America and Europe,* Lanham, MD: Rowman and Littlefield.
Landelijk Informatiesysteem Schulden (2009) *Protocol 'Landelijk Informatiesysteem Schulden ter voorkoming van problematische schulden'.*
Latour, B. (1992) 'Where are the missing masses? The sociology of a few mundane artifacts', blz. 226-258 in W. Bijker & J. Law (red.) *Shaping technology/building society*, Cambridge, MA: MIT Press.
Latour, B. (2005) *Reassembling the social. An introduction to actor-network-theory,* Oxford: Oxford University Press.
Leadbeater, C. (2008) We-think: Mass innovation, not mass production, London: Profile.

Leenes, R., B.J. Koops & L. van der Wees (2010) *Onderzoek naar het gebruik van het Burgerservicenummer (BSN) binnen de keten van de elektronische dienstverlening tussen de overheid en bedrijven. Onderzoek in opdracht van het Ministerie van EZ*, Den Haag, 16 juli 2010.

Lenk, K. & R. Traunmüller (2007) 'Broadening the concept of electronic government' in *Designing e-government*, The Hague/Boston: Kluwer Law International 2007.

Leukfeldt, E.R., M.M.L. Domenie & W.Ph. Stol (2010) *Verkenning Cybercrime in Nederland 2009*, Veiligheidsstudies. Den Haag: Boom Juridische Uitgevers.

Levin, A. & P. Sánchez Abril (2009) 'Two notions of privacy online', *Vanderbilt Journal of Entertainment and Technology Law* 11, 4: 1001-1051.

Liberatore, A. (2005) *Balancing security and democracy: the politics of Biometric Identification in the European Union*, EUI Working Papers, RSCAS no. 2005/30.

Liebenau, J. & J. Backhouse (1990) *Understanding information: An introduction*, Londen: Macmillan.

Lips, M.S. van der Hof, J.E.J. Prins, A.A.P. Schudelaro & M. de Vries (2005) *Issues of online personalisation and commercial and public service delivery*. Nijmegen: Wolf Legal Publishers, 2005.

Lips, A.M.B., J.A. Taylor & J. Organ (2009) 'Service transformation towards citizen-centric Government? The evolution of a smart card application in UK local Government', blz. 66-82 in A.J. Meijer, K. Boersma & P. Wagenaar (red.) *ICTs, citizens en governance: After the hype*!, Amsterdam: IOS Press Series 'Innovation and the public sector'.

Loon, M. van (2010) *Goed opdrachtgeverschap jegens ICTU*, WRR-webpublicatie nr. 50, www.wrr.nl.

Lor, P. & J. Britz (2007) 'Is a knowledge society possible without freedom of access to information?', *Journal of Information Science* 33, 4: 387-397.

Lubbe, J.C.A. van der (2002) 'Van een informatie- naar een kennismaatschappij. De rol van techniek', blz. 31-116 in H. Dijstelbloem & C.J. Schuyt (red.) *De publieke dimensie van kennis*, Den Haag: Sdu uitgevers.

Luhmann, N. (1979) *Trust and Power*, H. Davis (transl.), New York: Wiley.

Lyon, D. (1994) *The electronic eye. The rise of surveillance society*, Cambridge: Polity Press.

Lyon, D. (2003) *Surveillance after September 11*. Cambridge: Polity Press.

Lyon, D. (2007) *Surveillance studies. An overview*, Cambridge: Polity Press.

Lyon, D. (2009) *Identifying citizens. ID cards as surveillance*, Cambridge: Polity Press.

MacGillavry, E.C. (2000) *Meewerken aan strafvordering door banken en Internet Service Providers. Een onderzoek naar wetgeving en praktijk*, Gouda: Quint.

MacKenzie, D.A. & J. Wajcman (red.) (1985) *The social shaping of technology*, Milton Keynes: Open University Press.

MacKenzie, D.A. (1999a) 'The certainty trough', blz. 43-46 in W.H. Dutton (red.) *Society on the line. Information politics in the digital a*ge, Oxford: Oxford University Press.

MacKenzie, D.A. (1999b) 'Technological determinism', blz.39-41 in W.H. Dutton (red.) *Society on the line. Information politics in the digital a*ge, Oxford: Oxford University Press.

Maes, R. (2003) 'Informatiemanagement in kaart gebracht', *PrimaVera Working Paper 2003-02,* Amsterdam: Universiteit van Amsterdam.

Magnet, S. (2009) 'Using biometrics to revisualize the Canada-US border', blz. 359-376 in I. Kerr et al. (red.) *Lessons from the identity trail. Anonymity, privacy and identity in a networked society*, Oxford: Oxford University Press.

Mansell, R. & R. Silverstone (red.) (1996) *Communication by design: The politics of information and communication technologies*, Oxford: Oxford University Press.

Marx, G. (2001) 'Identity and anonymity: some conceptual distinctions and issues for research', blz. 311-327 in J. Caplan & J. Torpey (red.) *Documenting individual identity. The development of state practices in the modern world,* Princeton: Princeton University Press.

Mayer-Schönberger, V. & D. Lazer (2007) 'From electronic government to information government' in V. Mayer-Schönberger and D. Lazer (red.) *Governance and information technology: from electronic government to information government,* Massachusetts: MIT Press.

Mayer-Schönberger, V. (2009) *Delete. The virtue of forgetting in the digital age*, Princeton: Princeton University Press.

Meijer, A. (2004) *Vreemde ogen dwingen. De betekenis van internet voor maatschappelijke controle in de publieke sector*, Den Haag: Boom Juridische Uitgevers.

Meijer, A. (2009) 'Informatietechnologie en verantwoordelijkheid: een onbeheersbare migratiemachine', blz. 157-190 in H. Dijstelbloem & A. Meijer (red.) *De Migratiemachine. De rol van technologie in het Migratiebeleid*, Amsterdam: Van Gennep.

Meijer, A., G.J. Brandsma & S. Grimmelikhuijsen (2010) 'Transparantie als fictieve verantwoording', *Bestuurswetenschappen* 4: 8-27.

Meijer, A. (2011) 'Overheidsverantwoordelijkheid in het informatietijdperk: een pleidooi voor het creëren van genormeerde experimenteerruimte' in D. Broeders, C.M.K.C. Cuijpers & J.E.J. Prins (red.) *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (1998) *Actieprogramma Elektronische Overheid. Een efficiëntere en effectievere overheid op de elektronische snelweg*, Den Haag.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2000) *Contract met de Toekomst*, *een visie op de elektronische relatie overheid-burger*, Den Haag.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2010) *Staat van het bestuur 2010*, Den Haag.

Ministerie van Economische Zaken et al. (1999) *Digitale Delta. Nederland online*, Den Haag.

Ministerie van Economische Zaken (1994) *Nationaal Actieprogramma Elektronische Snelwegen*, Den Haag.

Ministerie van Economische Zaken (2008) *ICT Agenda 2008-2011. De gebruiker centraal in de digitale dienstenmaatschappij*, Den Haag, juni 2008.

Ministerie van Justitie (2010) *Visie op biometrie in de identiteitsketen publieke sector*, Den Haag, Programma VIPS, juli 2010.

Ministerie van Sociale Zaken en Werkgelegenheid (2010) *Strategische Kennisagenda editie 2010,* Den Haag.

Ministerie van Sociale Zaken en Werkgelegenheid & Ministerie van Volksgezondheid Welzijn en Sport (2010) *Programma Stroomlijning Indicatieprocessen in Zorg en Sociale Zekerheid 2006-2009*, Den Haag.

Mitrakas, A. (1997) *Open EDI and law in Europe,* The Hague: Kluwer Law International.

Mitsilegas, V. (2009) 'The Borders Paradox. The surveillance of movement in a union without internal frontiers', blz. 33-64 in H. Lindahl (red.) *A right to inclusion and exclusion? Normative faultlines of the EU's area of freedom, security and justice*, Oxford: Hart.

Mom, P. (2010) 'Zesje voor midoffice Logica', *Automatiseringsgids*, 23 april.

Monahan, T. (red.) (2006) *Surveillance and security. Technological politics and power in everyday life,* London: Routledge.

Mul, J. de, E. Müller & A. Nusselder (2001) *ICT de baas? Informatietechnologie en menselijke autonomie,* Onderzoeksprogramma Internet en Openbaar Bestuur, Den Haag.

Mul, J. de (2003) *Cyberspace Odyssee*, Kampen: Klement.

Mul, J. de (2010) 'Keuzedelirium: Over de paradox van de keuzevrijheid', *Database Delirium*, Amsterdam: Bert Bakker.

Mulder, K.F. (2006) 'Managing the dynamics of technology in modern day society', blz. 109-130 in R.M. Verburg et al. (red.) *Managing technology and innovation, an introduction,* New York: Routledge.

Mulgan, R. (2000) 'Accountability': An ever-expanding concept?', *Public Administration* 78, 3: 555-572.

Müller-Wille, B. (2008) 'The effect of international terrorisme on EU Intelligence Co-Operation', *JCMS* 46, 1: 49-74.

Nass, C., J. Steuer & E. Tauber (1994) 'Computers are social actors', *Human Factors in Computing Systems*, april: 72-78.

Nass, C., Y. Moon, B. Fogg, B. Reeves & D. Dryer (1995) 'Can computer personalities be human personalities?', *Human-Computer Studies* 43: 223-229.

Nationaal Uitvoeringsprogramma Dienstverlening en e-overheid (2008) *Nationaal Uitvoeringsprogramma Dienstverlening en e-Overheid: Burger en bedrijf centraal*, 1 december 2009, te raadplegen op www.e-overheid.nl.

Nationale Ombudsman (2008) rapport 2008/242, Den Haag.

Nationale Ombudsman (2009a) *De burger in de ketens. Verslag van de Nationale Ombudsman over 2008*, Den Haag.

Nationale Ombudsman (2009b), rapport 2009/015, Den Haag.

Nationale Ombudsman (2010a) *Toets een 1…, toets een 2…, toets een 3… Wat kan ik voor u doen? Een onderzoek naar de telefonische dienstverlening door de overheid*, rapport 2010/010, Den Haag.

Nationale Ombudsman (2010b) *Voorbij het conflict. Verslag van de Nationale Ombudsman over 2009*, Den Haag.

Nationale Ombudsman (2010c) *Toegang verboden. Onderzoek naar de opname van vreem-*

delingen in het Schengen Informatie Systeem en de informatievoorziening hierover, rapport 2010/115, Den Haag.

Naughton, J. (2010a) 'The internet: Everything you ever need to know', *The Observer*, 20 juni 2010.

Naughton, J. (2010b) 'Live with the WikiLeakable world or shut down the net. It's your choice', *The Guardian*, 6 december 2010.

Neuman, L. & R. Calland (2007) 'Making the law work: The challenges of implementation' in A. Florini (red.) *The right to know*, Chichester: Columbia University Press.

Noordegraaf, M., A.B. Ringeling & F.J.M. Zwetsloot (red.) (1995) *De ambtenaar als publiek ondernemer*, Bussum: Countinho.

NRC *Next* (2010) 'Pats, boem. En geen sporen. Maar de auto vertelt meer', 26 april 2010.

Nussbaum, M.C. (2000) 'The costs of tragedy: Some moral limits of cost-benefit analysis', *The Journal of Legal Studies* 29, S2: 1005-1036.

Nusselder, A. (2007) 'The virtual ego and the cyborg', *Journal of European Psychoanalysis* 25, 2. http://www/psychomedia.it/jep/number25/nusselder.htm, geraadpleegd op 17 augustus 2010.

OECD (2008) *OECD information technology outlook 2008*, Paris.

Olsthoorn, P. (2010) *De macht van Google,* Utrecht: Kosmos Uitgevers.

Osborne, D. & T. Gaebler (1992) *Reinventing government: How the entrepreneurial spirit is transforming the public sector,* Reading: Addison Wesley.

Oudshoorn, N. & T. Pinch (red.) (2003) *How users matter: The co-construction of users and technology*, Cambridge, MA: MIT Press.

Overkleeft-Verburg, G. (2009) 'Basisregistraties en rechtsbescherming. Over de dualisering van de bestuursrechtelijke rechtsbetrekking', *Nederlands Tijdschrift voor Bestuursrecht* 2009, nr. 4.

Palfrey, J. & U. Gasser (2008) *Born digital. Understanding the first generation of digital natives*, New York: Basic Books.

Petri, G. (2008) 'Clinger-Cohen Act voorbeeld voor Nederlandse overheid', *Automatisering Gids*, nr. 8, Den Haag: Sdu Uitgevers.

Pinch, T. J. & W.E. Bijker (1984) 'The social construction of facts and artefacts: or how the sociology of science and technology might benefit each other', *Social Studies of Science* 14: 399-441.

Pluut, B. (2010) *Het landelijk EPD als blackbox*, WRR-webpublicatie nr. 45, www.wrr.nl.

Porter, M.P. (1995) *Trust in numbers. The pursuit of objectivity in science and public life,* Princeton: Princeton University Press.

Posner, R.A. (1984) 'An economic theory of privacy', blz. 333-345 in F.D. Schoeman (red.) *Philosophical dimensions of privacy: An anthology*, Cambridge: Cambridge University Press.

Potters, P. & M. de Vreeze (2010) eCall Blackbox. WRR-webpublicatie nr. 48, www.wrr.nl.

Power, M. (2005) 'The theory of the audit explosion', blz. 326-344 in E. Ferlie et al. (red.) *The Oxford handbook of public management*, Oxford: Oxford University Press.

Prins, J.E.J. (2007) 'Technocratie en de toekomstagenda van de Nationale Ombudsman', blz. 111-134 in *Werken aan behoorlijkheid. De Nationale Ombudsman in zijn context*

(jubileumbundel 25 jaar Nationale Ombudsman), Den Haag: Boom Juridische Uitgevers.
Prins, J.E.J. (red.) (2007) *Designing e-government*, The Hague: Kluwer Law International.
Prins, J.E.J. (2009) 'Name, shame and everlasting blame', *Nederlands Juristenblad* 84, 3: 119.
Prins, J.E.J. (2010a) 'Burgers en hun privacy: over verhouding en houding tot een ongemakkelijk bezit', blz.1-14 in J.E.J. Prins et al. (red.) *16 miljoen BN'ers? Bescherming van persoonsgegevens in het Digitale Tijdperk*, Leiden: Stichting NJCM-Boekerij.
Prins, J.E.J. (2010b) 'Discriminatiesignalen' *Nederlands Juristenblad* 85, 2: 59.
Raad van Hoofdcommissarissen (2005) *Politie in ontwikkeling*.
Raad van Hoofdcommissarissen (2009) *Beelden van de Samenleving. Visie op cameratoezicht in een netwerksamenleving*.
Raad van State (2009) *Jaarverslag over 2008,* Den Haag.
Raad van State (2010) *Jaarverslag over 2009,* Den Haag.
Raad voor Cultuur & Raad voor het Openbaar Bestuur (2008) *Informatie: grondstof met toekomstwaarde. Contouren van een visie op de rol en betekenis van informatie*, Den Haag.
Raad voor het Openbaar Bestuur (1998) *Dienen en verdienen met ICT. Over de toekomstige mogelijkheden van de publieke dienstverlening*, Den Haag.
Raad voor het Openbaar Bestuur (2010a) *Vertrouwen op democratie,* Den Haag.
Raad voor het Openbaar Bestuur (2010b) *Het einde van het blauwdruk-denken. Naar een nieuwe inrichting van het openbaar bestuur*, Den Haag.
Rathenau Instituut (1998) *Persoonsgegevens in de informatiemaatschappij.* Berichten aan het Parlement, Den Haag: Rathenau Instituut.
Rathenau Instituut, de Consumentenbond en ECP.nl (2007) *RFID bewustzijn van consumenten: Hoe denken Nederlanders over Radio Frequency Identification?*, Den Haag.
Rathenau Instituut (2008) *Midden in de maatschappij*, Jaarverslag 2007, Den Haag.
Rathenau Instituut (2010) *Wat is dat eigenlijk, menselijk leven?,* Jaarverslag 2009, Den Haag: http://epub02.publitas.nl/36/2/magazine.php#/spreadview/18/, geraadpleegd op 11 september 2010.
Reding, V. (2010) *The challenges ahead for the European Union*, Keynote Speech at the Data Protection Day 28 January 2010, European Parliament, Brussels.
Reeves, B. & Clifford Nass (1996) *The media equation*, Cambridge: Cambridge University Press.
Regeerakkoord (2010) *Vrijheid en Verantwoordelijkheid. Regeerakkoord VVD-CDA*, Den Haag.
Rijksarchiefinspectie (2005) *Dementerende Overheid*, Den Haag.
Rijksdienst voor het Wegverkeer (2008) *Chip op het rijbewijs,* Verkenning versie 2.1, Den Haag.
RINIS (2010) *RINIS Actueel*, juni 2010.
Robinson, N. et al. (2010) *Security, at what cost? Quantifying people's trade-offs across liberty, privacy and security*, Cambridge: RAND Europe.
Ronfeldt, D. (1992) 'Cyberocracy is coming', *Information Society* 8: 243-296.

Rozemond, K. (2010) 'De droom van Beccaria. Over het strafrecht en de nodale veiligheidszorg', *Rechtsfilosofie en Rechtstheorie* 2010, 2: 158-175.

Schenk-Geers, A.C.M. (2007) *Internationale fiscale gegevensuitwisseling en de rechtsbescherming van de belastingplichtige*, dissertatie, Tilburg.

Schermer, B.W & T. Wagemans (2009) *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat*, Considerati, in opdracht van CBP.

Schinkel, W. (2009) 'De nieuwe preventie. Actuariële archiefsystemen en de nieuwe technologie van veiligheid', *Krisis. Tijdschrift voor Actuele Filosofie*, 2: 1-21.

Schravendeel, D. & S. Luitjens (2001) 'Een vernieuwde gegevenshuishouding voor de overheid. Doelstelling, inhoud en werkwijze van het programma Stroomlijning Basisgegevens', blz. 347-362 in H. van Duivenboden & M. Lips (red.) *Klantgericht werken in de publieke sector. Inrichting van de elektronische overheid*, Utrecht: Lemma.

Schreijenberg, A., J. Koffijberg & S. Dekkers (2009) *Eindrapport Evaluatie cameratoezicht op openbare plaatsen*, Amsterdam: Regioplan.

Schwartz, B. (2004) *The paradox of choice. Why more is less. How the culture of abundance robs us of satisfaction*, New York: Harper Collins.

Scott, J. (1998) *Seeing like a state. How certain schemes to improve the human condition have failed,* New Haven: Yale University Press.

Sheptycki, J. (2007) 'Transnational crime and transnational policing', *Sociology Compass* 1, 2: 485-498.

Shrader-Frechette, K. (1992) 'Technology, Bayesian policymaking, and democratic process', blz. 123-137 in L. Winner (red.) *Democracy in a technological society*, Dordrecht: Kluwer.

Silverstone, R. & E. Hirsch (red.) (1992) *Consuming technologies: Media and information in domestic spaces*, New York: Routledge.

Simon, H. (1956) 'Rational choice and the structure of the environment', *Psychological Review* 63: 129-138.

Singh, S. (2007) 'Grassroots initiatives' in A. Florini (red.) *The right to know,* Chichester: Columbia University Press.

Snellen, I. (1992) 'Het Nederlandse parlement in een geïnformatiseerde samenleving', blz. 301-318 in P. Frissen et al. (red.) *Orwell of Athene. Democratie en informatiesamenleving*, Den Haag: Sdu.

Snellen, I. (1994) 'De revolutionaire werking van informatie- en communicatietechnologie in het openbaar bestuur', blz. 417-432 in A. Zuurmond et al. (red.) *Informatisering in het openbaar bestuur. Technologie en sturing bestuurskundig beschouwd,* Den Haag: VUGA.

Snellen, I. (2005) 'E-Government. A challenge for public management', blz. 398-421 in E. Ferlie et al. (red.) *The Oxford handbook of public management*, Oxford: Oxford University Press.

Snijder, M. (2011) *Het biometrische paspoort in Nederland: crash of zachte landing*, WRR-webpublicatie nr. 51, www.wwr.nl.

Snijders, T. (2011) 'Chief Information Officers bij de Rijksoverheid', in D. Broeders,

C.M.K.C. Cuijpers & J.E.J. Prins (red) *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press.

Sociaal en Cultureel Planbureau (2004) *In het zicht van de toekomst*, Den Haag.

Sociaal en Cultureel Planbureau (2008) *Sociale veiligheid ontsleuteld. Veronderstelde en werkelijke effecten van veiligheidsbeleid*, Den Haag.

Socialistische Partij (2008) *ICT bij de overheid, wondermiddel of hoofdpijndossier?,* http://www.sp.nl/service/rapport/080704_ictbijdeoverheid.pdf

Solove, D.J. (2004) *The digital person*, New York: New York University Press.

Solove, D. (2007) *The future of reputation, gossip, rumor and privacy on the internet*, New Haven, CT: Yale University Press.

Solove, D.J. (2008) *Understanding Privacy*, Cambridge, MA: Harvard University Press.

Staatscommissie Grondwet (2010) *Rapport Staatscommissie Grondwet*, Den Haag.

Stevens, B. (2004) 'The emerging security economy: An introduction' in OECD, *The Security Economy*, Paris: OECD.

Stevens, T., J. Elliott, A. Hoikkanen, I. Maghiros & W. Lusoli (2010) *The state of the electronic identity market: Technologies, infrastructure, services and policies*, JRC Scientific and Technical Reports, Luxembourg: Publications Office of the European Union.

Stirling, A. (2008) 'Opening up' and 'closing down' *Science, Technology and Human Values* 33, 2: 262-294.

Straten, G.F.M. (1996) *In de beslotenheid van het openbaar bestuur. De institutionalisering van informatietechnologie binnen de bevolkingsadministratie*, Utrecht.

Tadros, V. (2006) 'Power and the value of privacy', blz. 105-120 in E. Claes et al. (red.) *Privacy and the criminal law*, Antwerpen: Intersentia

Taylor, J.R. & E.J. van Every (1993) *The vulnerable fortress. Bureaucratic organization and management in the information age,* Toronto: Toronto University Press.

Teeuw, W.B. & A.H. Vedder (red.) (2008) *Security applications for converging technologies. Impact on the constitutional state and legal order*, WODC.

Thaens, M. (1998) *De procesbenadering van ICT-evaluatie. De rol van evaluatie in het besluitvormingsproces over investeringen in informatie- en communicatietechnologie binnen een organisatie*, Delft: Eburon.

Tiemeijer W.L. (2006) *Het geheim van de burger: over staat en opinieonderzoek*, Amsterdam: Aksant.

Tiemeijer, W.L. (2009) 'Slotbeschouwing', blz. 293-311 in W.L. Tiemeijer, C.A. Thomas & H.M. Prast (red.) *De menselijke beslisser: Over de psychologie van keuze en gedrag*, WRR-verkenning nr. 22, Amsterdam: Amsterdam University Press.

TNO (2009) *Marktrapportage elektronische communicatie,* september 2009.

Torpey, J. (1998) 'Coming and going: on the state monopolization of the legitimate means of movement', *Sociological Theory* 16, 3: 239-259.

Torpey, J. (2000) *The invention of the passport; surveillance, citizenship and the state.* Cambridge: Cambridge University Press.

Trouw (2010) 'Australische politie start onderzoek naar Google', http://www.trouw.nl/nieuws/wereld/article3088346.ece/Australische_poli-

tie_start_onderzoek_naar_Google.html, geraadpleegd op 18 juni 2010.
Tsoukas, H. (1997) 'The tiranny of light. The temptations and the paradoxes of the information society', *Futures* 29, 9: 827-843.
Tweede Kamer (1999-2000) *Motie over bevordering van de ontwikkeling en het gebruik van Privacy Enhancing Technologies*, Kamerstukken II, 25892, nr. 31.
Tweede Kamer (1997-1998) *Nota wetgeving voor de elektronische snelweg*, Kamerstukken II, 25880, nr. 2.
Tweede Kamer (2000-2001a) *Verslag algemeen overleg op 21 juni 2001 over biometrie in reisdocumenten en elektronische identiteitskaart*, Kamerstukken II, 25764, nr. 17.
Tweede Kamer (2000-2001b) *Actieprogramma Elektronische overheid – Nota De elektronische overheid aan het begin van de 21e eeuw*, Kamerstukken II, 26387, nr. 9.
Tweede Kamer (2000-2001c) *Nota Kaderstellende visie op toezicht*, Kamerstukken II, 27831, nr. 1.
Tweede Kamer (2004-2005) *Brief inhoudend 'spoorboekje' voor implementatie EPD*, Kamerstukken II, 27529, nr. 15.
Tweede Kamer (2005-2006a) *Memorie van Toelichting Wet algemene bepalingen burgerservicenummer*, Kamerstukken II, 30312, nr. 3.
Tweede Kamer (2005-2006b) *Brief inzake modernisering van de overheid*, Kamerstukken II, 29362, nr. 101.
Tweede Kamer (2005-2006c) *Motie Slob – Wet algemene bepalingen burgerservicenummer*, 30312, nr. 15.
Tweede Kamer (2006-2007) *Brief inhoudend Voortgangsrapportage ICT in de zorg*, Kamerstukken II, 27529, nr. 29.
Tweede Kamer (2007-2008a) *Memorie van Toelichting bij wijziging Paspoortwet*, Kamerstukken II, 31324 (R1844), nr. 3 (herdruk).
Tweede Kamer (2007-2008b) *Brief inzake project Veiligheid begint bij voorkomen,* Kamerstukken II, 28684, nr. 119.
Tweede Kamer (2008-2009a) *Behandeling van het wetsvoorstel Wijziging van wet gebruik burgerservicenummer in de zorg*, Handelingen II, 31466, nr. 45, blz. 3920-3941.
Tweede Kamer (2008-2009b) *Behandeling van het wetsvoorstel Wijziging van wet gebruik burgerservicenummer in de zorg*, Handelingen II, 31466, nr. 45, blz. 3942-3959.
Tweede Kamer (2008-2009c) *Verslag algemeen overleg van 30-10-2008 over de software van de OV-chipkaart en deurpasjes*, Kamerstukken II, 23645, nr. 274.
Tweede Kamer (2008-2009d) *Brief minister over antiterrorismebeleid*, Kamerstukken II, 29754, nr. 164.
Tweede Kamer (2008-2009e) *Brief minister en staatssecretaris over advies 'Informatie: grondstof met toekomstwaarde'*, Kamerstukken II, 29362, nr. 156.
Tweede Kamer (2008-2009f) *Memorie van Toelichting – Wijziging van onder meer Boek 2 van Burgerlijk Wetboek en de Wet documentatie vennootschappen*, Kamerstukken II, 31948, nr. 3.
Tweede Kamer (2009-2010a) *Brief inzake modernisering GBA*, Kamerstukken II, 27859, nr. 38.
Tweede Kamer (2009-2010b) *Brief staatssecretaris over preventie en bestrijding van stille armoede en sociale uitsluiting*, Kamerstukken II, 24515, nr. 170.

Tweede Kamer (2009-2010c) *Informatiehuishouding van de politie*, Kamerstukken II, 29628, nr. 217.
Tweede Kamer (2009-2010e) *Wijziging van de Wet houdende wijziging van de Elektriciteitswet 1998 en de gaswet*, Kamerstukken II, 2009/10, 32374, nrs. 1-4.
Tweede Kamer (2009-2010f) *Evaluatie Wet bescherming persoonsgegevens*, Kamerstukken II, 2009/10, 31051, nr. 6.
Tweede Kamer (2009-2010g) *Brief inzake Voortgangsrapportage landelijke infrastructuur voor gegevensuitwisseling in de zorg*, Kamerstukken II, 27529, nr. 61.
Tweede Kamer (2009-2010h) *Wetsvoorstel overige fiscale maatregelen 2010,* Kamerstukken II, 32129, nr. 2.
Tweede Kamer (2009-2010i) *Brief inzake modernisering GBA,* Kamerstukken II, 27859, nr. 30.
Tweede Kamer (2009-2010j) *Kabinetsstandpunt advies Commissie Brouwer-Korf en evaluatie van de Wet bescherming persoonsgegevens*, Kamerstukken II, 31051, nr. 5.
Tweede Kamer (2009-2010k) *Brief inzake Modernisering van de overheid*, Kamerstukken II, 29362, nr. 157.
Tweede Kamer (2010-2011a) *Algemeen Overleg over Nederlandse reisdocumenten*, Kamerstukken II, 25764, nr. 44.
Tweede Kamer (2010-2011b) *Algemeen Overleg met de vaste Commissie voor Financiën*, 31066, nr. 95.
Tweede Kamer (2010-2011c) *Kabinetsreactie Digitale Agenda voor Europa*, Kamerstukken II, 21501-332, nr. 294.
Tweede Kamer (2010-2011e) *Fiche inzake doorgifte van PNR-gegevens,* Kamerstukken II, 22112, nr. 1081.
Tweede Kamer (2010-2011f) *Kentekenherkenning boven de A28*, Bijlage bij Kamerstukken 31051, nr. 8.
Tweede Kamer (2010-2011g) *Kamervragen over het ten onrechte opslaan van kentekengegevens van burgers*, 2010Z19218.
Verbeek, J.P.G.M. (2010) 'Grensoverschrijdende toegang tot politiële databases', blz. 29-34 in L.H.C. Bertram & D.H. van Ekelenburg (red.) *Opsporingsinformatie vrij verkrijgbaar in Europa?*, Deventer: Kluwer.
Verenigde Naties (2009) *From e-Government to connected Governance, United Nations e-Government survey 2008*, New York.
Verenigde Naties (2010) *Leveraging e-government at a time of financial and economic crisis, United Nations e-Government Survey 2010*, New York.
Vereniging van Nederlandse Gemeenten (2008) *Brief Vereniging van Nederlandse Gemeenten met een reactie op de conceptwetgeving Verwijsindex*, Den Haag, Nederlandse Vereniging van Gemeenten, 12 maart 2008.
Vereniging van Nederlandse Gemeenten (2010) *Thorbecke 2.0: naar een vernieuwde Nederlandse overheid*, VNG-discussienotitie 23 maart 2010, raadpleegbaar op www.vng.nl.
Verhey, L.F.M. (1992) *Horizontale werking van grondrechten, in het bijzonder het recht op privacy*, W.E.J. Tjeenk Willink.

Verhoeven, I. (2009) *Burgers tegen beleid. Een analyse van dynamiek in politieke betrokkenheid*, Amsterdam: Aksant.
VNO-NCW (2005) *Brief aan de leden van de Vaste Tweede Kamer Commissies voor Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Justitie*, Den Haag, 28 oktober 2005, http://www.eerstekamer.nl/behandeling/20080303/brief_van_vno_ncw_aan_de_tweede/f=/w30312ibijl2.pdf.
Volokh, E. (2000) 'Freedom of speech and information privacy: The troubling implications of a right to stop people from speaking about you', *Stanford Law Review* 52: 1049 ff.
Waldron, J. (2007) 'Is this torture necessary?', *The New York Review of Books* 54: 16 e.v. (25 oktober 2007).
Warren, S.D. & L.D. Brandeis (1890) 'The right to privacy', *Harvard Law Review* 4: 193ff.
Wetenschappelijke Raad voor het Regeringsbeleid (1998) *Staat zonder land. Een verkenning van bestuurlijke gevolgen van informatie- en communicatietechnologie*, Den Haag: Sdu Uitgevers.
Wetenschappelijke Raad voor het Regeringsbeleid (2002) *Van oude en nieuwe kennis. De gevolgen van ICT voor het kennisbeleid*, Den Haag: Sdu Uitgevers.
Wetenschappelijke Raad voor het Regeringsbeleid (2008a) *Innovatie vernieuwd: Opening in viervoud*, Amsterdam: Amsterdam University Press.
Wetenschappelijke Raad voor het Regeringsbeleid (2008b) *Onzekere veiligheid. Verantwoordelijkheden rond fysieke veiligheid*, Rapporten aan de regering nr. 82, Amsterdam: Amsterdam University Press.
Whitson, J. & K.D. Haggerty (2008) 'Identity theft and the care of the virtual self', *Economy and Society* 37, 4: 571-593.
Williams, R. & D. Edge (1996) 'The social shaping of technology', blz. 53-67 in W.H. Dutton (red.) *Information and communication technologies. Visions and realities,* Oxford: Oxford University Press.
Williams, R. (1999) 'The social shaping of technology', blz. 41-43 in W.H. Dutton (red.) *Society on the line. Information politics in the digital a*ge, Oxford: Oxford University Press.
Winter, H.B. et al. (2008) *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*, Den Haag: WODC.
Wisse, P. (2008) 'Semantiek, interoperabiliteit en infrastructuur', blz. 382-391 in S. Zwienink & P. Wisse (red.) *Eerlijk zullen we alles delen*, Den Haag: Forum Standaardisatie.
Witteveen, W.J. (2010) 'Kafka en de verbeelding van de bureaucratie', *RegelMaat* 25, 4: 218-226.
Woolgar, S. (1996) 'Technologies as cultural artefacts', blz. 88-102 in W.H. Dutton (red.) *Society on the line. Information politics in the digital a*ge, Oxford: Oxford University Press.
Wyatt, S. (2003) 'Non-users also matter', blz. 67-80 in N. Oudshoorn & T. Pinch (red.) *How users matter: The co-construction of users and technology*, Cambridge, MA: MIT Press.
Zedner, L. (2007) 'Pre-crime and post-criminology', *Theoretical Criminology*, vol. 11: 261-281.

Zenc (2007) *De toekomst van persoonsinformatiebeleid. Een dynamische kijk op privacy*, Rapport in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag

Zittrain, J. (2008) *The future of the internet. And how to stop it*, New Haven: Yale University Press.

Zouridis, S. (2000) *Digitale disciplinering. Over ICT, organisatie, wetgeving en het automatiseren van beschikkingen*, Delft: Eburon.

Zureik, E. & M. Salter (red.) (2005) *Global surveillance and policing. Borders, security, identity*, Collumpton: Willan Publishing.

Zuurmond, A. (1994) *De infocratie. Een theoretische en empirische heroriëntatie op Weber's ideaaltype in het informatietijdperk,* Den Haag: Pheadrus.

Zuurmond, A. & M. Meesters (2005) 'ICT en overheidsorganisatie', blz. 299-327 in M. Lips et al. (red.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Lemma.

Zwenne, G.J. (1998) *Belastingheffing en informatieverplichtingen. Reikwijdte en begrenzing van informatiebevoegdheden in de verhouding tussen belastingdienst en banken*, Den Haag: Sdu.

Zwenne, G.J., A. Dutler, M. Groothuis, H. Kielman, W. Koelewijn & L. Mommers (2007) *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse*, Den Haag: WODC.

LIJST VAN GESPROKEN PERSONEN

Functieaanduidingen ten tijde van het interview

Mevr. K. Aarde, ministerie van Justitie, Helpdesk Privacy
Dhr. R. Adams, Rijkswaterstaat
Dhr. S. Arjun Sharma, ministerie van BZK
Dhr. J. Attema, ECP-EPN
Dhr. Marcel van Asperdt, Nationaal Bureau voor Verbindingsbeveiliging
Dhr. R. Barth, PrivacyBarometer
Dhr. R.H. van de Beeten, lid Eerste Kamer
Dhr. prof. V.J.J.M. Bekkers, hoogleraar informatie- en communicatietechnologische infrastructuren in de publieke en private sector, Erasmus Universiteit Rotterdam
Dhr. A. van Bellen, directeur ECP-EPN
Mevr. B. van den Berg, Universiteit van Tilburg
Dhr. L. Beslay, bureau European Data Protection Supervisor, Brussel
R.O. Blad, ministerie van EZ
Mevr. E.Y. Bogerman, directeur ICTU
Dhr. M. Bolhuis, European Privacy Officer Google Nederland
Mevr. S. Borgers, CIO bij ministerie van VROM
Dhr. L. Bos, voorzitter ICMCC en redacteur patientenepd.nl
Dhr. M. Bouten, ICTU
Mevr. d. Boyd, Microsoft Research & Harvard University, Verenigde Staten
Dhr. A.F.M. Brenninkmeijer, Nationale Ombudsman
Dhr. R. Broekens, consultant Verdonck Klooster & Associates
Dhr. prof. W.A. Brom, Rathenau Instituut
Dhr. I. Brown, Oxford Internet Institute
Dhr. M. Brugman, ICTU
Dhr. T. de Bruijn, Permanente Vertegenwoordiger bij de EU, Brussel
Dhr. F. Buijnsters, student en initiatiefnemer epd-nee.nl
Dhr. F. Bussemaker, Program Manager WCIT2010 Amsterdam
Dhr. L. Bygrave, Universiteit van Oslo
Dhr. L. Cok, ICTU
Dhr. N.P. Coleman, Permanente Vertegenwoordiging bij de EU, Brussel
Dhr. O. van Daalen, Bits of Freedom
Dhr. P. van Dalen, vreemdelingenpolitie Brabant Zuid-Oost
Dhr. R. van Dam, CapGemini
Mevr. N. Damen, projectleider VIR departement Jeugd en Gezin
Dhr. C. Dekker, huisarts te Urk en lid van comité ‘wake-up’
Dhr. E.J. Delwel, vtspn Politie Nederland, Programmamanager implementatie Progis (Programma Informatievoorziening Strafrechtsketen)
Dhr. P. Diederen, Adviesraad voor het Wetenschaps- en Technologiebeleid

Dhr. J. Dijkstra, Nederlands Normalisatie-instituut (NEN)
Dhr. J.A. Dijkstra, NEN-Elektro & ICT
Dhr. J.W. van Dongen, Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR)
Dhr. H. Donkhorst, Belastingdienst
Dhr. E. van Doorn, consultant Verdonck Klooster & Associates
Dhr. B. Drewes, coördinator Informatiebeleid, Vereniging van Nederlandse Gemeenten
Dhr. N. Ducastel, Het Expertise Centum
Dhr. C. van Duijvenvoorden, CIO bij ministerie van AZ
Dhr. J.W. Duijzer, CIO bij ministerie van LNV
Dhr. prof. H. van Duivenboden, b&a Consulting/hoogleraar informatisering en interbestuurlijke samenwerking Universiteit van Tilburg
Dhr. prof. S. Dutta, Academic Director eLab, INSEAD, Fontainebleau, Frankrijk
Dhr. prof. W. Dutton, Directeur Oxford Internet Institute
Mevr. C. Ebbers, privacy consultant
Mevr. P. van den Eijnden, ministerie van BZK
Dhr. S. Eilander, directeur Faciliteiten-, Huisvesting- en Inkoopbeleid bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Mevr. A.C.J.M. Emmaneel, senior beleidsmedewerker College Bescherming Persoonsgegevens (CBP)
Dhr. A. van Ess, Voelspriet.nl
Dhr. R van Est, Rathenau Instituut
Dhr. P. van der Feltz, Country Manager Google Nederland
Dhr. B. Filippini, PrivacyFirst
Dhr. J. Flippo, CIO bij ministerie van BZ
Dhr. prof. H. Franken, Eerste Kamer/hoogleraar Informatierecht, Universiteit Leiden
Dhr. E. Frinking, Centrum voor Strategische Studies
Mevr. prof. V.A.J. Frissen, TNO/hoogleraar ICT en sociale verandering, Erasmus Universiteit Rotterdam
Mr. H. Gardeniers, directeur/adviseur Net2Legal privacyadvies
Dhr. B. Garnier, senior beleidsadviseur ICT-beleid voor het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Dhr. M. van Gelderen, ministerie van V&W
Dhr. L. Geluk, wethouder Jeugd, Gezin en Onderwijs Rotterdam
Mevr. A. Gerkens, lid Tweede Kamer voor de SP
Dhr. prof. R. van Gestel, hoogleraar Wetgeving en Methodieken, Universiteit van Tilburg
Dhr. H. Grevelman, directeur Technologie & Implementatie ZwitserLeven/lid CIO-overleg
Dhr. H. van Grieken, CapGemini
Dhr. S. van Grieken, Stichting Het Nieuwe Stemmen
Dhr. prof. J.H.A.M. Grijpink, Raadsadviseur ministerie van Justitie/Universiteit Utrecht
Dhr. M. de Groot, OBA MileStones
Dhr. F.J. van der Haar, VH Groningen
Dhr. Habets, bestuurslid LHV (portefeuille ICT en vice-voorzitter) en huisarts

Dhr. S. van Haersema Buma, lid Tweede Kamer voor het CDA
Dhr. P. Hagedoorn, partner 3Align Information Governance/lid CIO-overleg
Dhr. J. Hakkenberg, directeur Rijksdienst voor het Wegverkeer, Lid ICTU stichtingsbestuur, voorzitter van de Manifestgroep
Dhr. J. Hamel, lid Eerste Kamer
Dhr. J. Van Hattum, Rijkswaterstaat
Mevr. E. Havenaar, manager Strategie en Externe betrekkingen, Nictiz
Dhr. G. Heimeriks, Adviesraad voor het Wetenschaps- en Technologiebeleid
Dhr. M. Heldoorn, beleidsmedewerker eHealth, NPCF
Mevr. J. Hennis-Plasschaert, lid Tweede Kamer voor de VVD
Dhr. H. Hijmans, bureau European Data Protection Supervisor, Brussel
Dhr. M.W.I. Hillenaar, directeur Informatiseringsbeleid/RijksCIO, ministerie van BZK
Dhr. J. Hoekman, Openbaar Ministerie
Mevr. S. van der Hof, Universitair hoofddocent TILT
Dhr. G.-P. van 't Hoff, Multisignaal
Dhr. V. Homburg, EUR
Dhr. C.G. van der Hoog, Privacy First
Dhr. Th. Hooghiemstra, Het Expertise Centrum
Dhr. prof. R. Hoppe, hoogleraar management en bestuur, Universiteit Twente
Dhr. prof. E. Huizer TNO directeur Kennis/ hoogleraar Informatiekunde, Universiteit Utrecht
Dhr. P. Hustinx, European Data Protection Supervisor, Brussel
Dhr. M. Jaber, ICTU programmamanager voor GovUnited
Dhr. prof. B.P.F. Jacobs, Hoogleraar *Software Security and Correctness,* Radboud Universiteit Nijmegen
Dhr. R. Jagt, bedrijfsjurist ICTU
Dhr. P. Jansen, beleidsmedewerker, NHG
Dhr. R. Jansen, ICTU programmamanager 'e-overheid voor burgers'
Mevr. J.B. de Jong, Ministerie van Justitie
Mevr. E. Jongeneel, Ketenmanager Veiligheidshuis Utrecht
Dhr. prof. W. Jonker, Philips Research Europe/ hoogleraar databasetechnologie in telematica-applicaties, Universiteit Twente
Dhr. P. de Kam, Senior consultant HEC
Dhr. N. Kaptein, CapGemini
Mevr. A. ten Kate-Schoots, Bedrijfsjuriste ICT~Office
Dhr. S. Katus, Nederlandse Spoorwegen
Dhr. W. Kegel, GBO.Overheid (nu Logius)
Dhr. M.E.M. Kerkvliet, Algemene Rekenkamer
Dhr. K. Keuzenkamp, plaatsvervangend directeur Dienstverlening, Regeldruk en Informatiebeleid
Dhr. H. Klap, Politie (vtspn), Programma Cybercrime, Raad van Hoofdcommissarissen
Dhr. G. Klei, privacyloket/ OBA MileStones BV
Dhr. R. Kleijmeer, De Nederlandsche Bank

Dhr. T. de Klerk, Stadsregio Rotterdam
Dhr. F. Knopjes, ID Management Centre/ministerie van Justitie
Dhr. E. Koedam, vtspn Politie Nederland
Dhr. J. Kohnstamm, voorzitter College Bescherming Persoonsgegevens
Dhr. L. Kok, ICTU
Dhr. B. Kokkeler, senior adviseur, ministerie van Landbouw, Natuur & Voedselkwaliteit
Dhr. H. Kooij, ECID
Dhr. H.R. Kranenborg, bureau European Data Protection Supervisor, Brussel
Dhr. F. Krom, CIO bij ING/lid CIO-overleg
Mevr. N. Kroon, ministerie van EZ
Dhr. J. Kuipéri, ICTU directielid
Dhr. J. Kuipers, Surfnet
Dhr. F. Kuitenbrouwer, journalist NRC *Handelsblad* en privacydeskundige
Mevr. L. Lap, projectmedewerker i-visie, Landbouw, Natuur & Voedselkwaliteit
Mevr. M. Laqueur, plaatsvervangend CIO, ministerie van Volksgezondheid, Welzijn en Sport
Dhr. M. Leenaars, Internet Society Nederland
Dhr. prof. dr. R.E. Leenes, Hoogleraar TILT, Universiteit Tilburg
Mevr. L. de Leeuw, Siemans IT Solutions & Services
Dhr. M. Levering, ECID
Dhr. S. Luijtjens, Gemeenschappelijke Beheersorganisatie Overheid
Dhr. T.H. van der Maas, adjunct-directeur ECP-EPN
Mevr. E. Maat, programmadirecteur Innovatie en ICT, ministerie van VWS
Dhr. E. MacGillavry, wetenschappelijk bureau Openbaar Ministerie
Dhr. H.C. Maduro, Staatsraad van het Koninkrijk, Raad van State
Dhr. prof. R. Maes, hoogleraar Informatiemanagement Universiteit van Amsterdam
Mevr. prof. H. Margetts, Oxford Internet Institute
Dhr. prof. V. Mayer-Schönberger, Oxford Internet Institute
Dhr. T. Mekel, directeur Business Development en ICT Athlon Car Lease/lid CIO-overleg
Mevr. prof. P.L. Meurs, lid Eerste Kamer/hoogleraar Bestuur van de Gezondheidszorg, EUR
Dhr. prof. V. Mitsilegas, Professor of European Criminal Law, Queen Mary University of London
Dhr. J. Moelker, programmamanager GBA voor het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Mevr. J. Moerman, CapGemini
Dhr. P. Mom, freelancejournalist op het gebied van e-overheid
Dhr. L. Mommers, consultant Legal Intelligence
Dhr. H. Moraal, Openbaar Ministerie
Dhr. J. Morijn, ministerie van BZK
Dr. ir. G. Munnichs, Rathenau Instituut
Dhr. R. van Munster, TNO, NBF
Dhr. G.H.M. Nielander, Centraal Bureau voor de Statistiek
Dhr. G. van 't Noordende, Universiteit van Amsterdam

Dhr. S. Nouwt, Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst
Dhr. P. Omtzigt, lid Tweede Kamer, CDA
Mevr. Ch. Van Ooijen, promovendus TILT, Universiteit van Tilburg
Dhr. T. van Oosterhout, Algemeen Projectleider GCOS
Dhr. M. Oosting, Staatsraad van het Koninkrijk, Raad van State
Dhr. C. van Oranje, Kabinet van Commissaris Kroes (Digitale Agenda), Brussel
Dhr. D. van Oudheusden, De Nederlandsche Bank
Dhr. G. Paalman, Sagem Identification
Dhr. B. Papenhuijzen, CIO bij ministerie van Justitie
Dhr. F. Paul, hoofd afdeling Large-Scale IT Systems, DG Justitie, Europese Commissie
Dhr. W. Pedroli, ministerie van BZK, Constitutionele Zaken
Dhr. S. Peereboom, directoraat-generaal Belastingdienst, ministerie van Financiën
Dhr. M. Poelmans, ministerie van BZK
Dhr. J.K.T. Postma, lid auditcommissies in de Rijksdienst
Dhr. P. Provily, ministerie van Buitenlandse Zaken
Dhr. M. Raijmakers, Raad van State
Dhr. H. Rauch, Principal Consultant CapGemini
Dhr. P. Reimer, juridisch adviseur Constitutionele Zaken (BZK)
Dhr. R. Rinzema, advocaat/partner Stibbe Advocaten
Dhr. A.P.C. Roosendaal, promovendus TILT, Universiteit van Tilburg
Mevr. H.J.Th.M. van Roosmalen, Raad van State
Dhr. R. Roozendaal, CIO bij ministerie van Volksgezondheid, Welzijn en Sport
Mevr. E. Rossieau, Openbaar Ministerie, projectsecretaris Intensiveringsprogramma Cybercrime
Dhr. A. Ruifrok, Nederlands Forensisch Instituut
Mevr. prof. M.A. Sasse, hoogleraar Human-Centred Technology University College London
Dhr. M. Savelkoul, ketenregisseur Identiteitsfraude ministerie van BZK
Dhr. P. van Schelven, bedrijfsjurist ICT~Office
Mevr. A. Schipaanboord, directeur beleid & innovatie, NPCF
Dhr. R. Schonck, voorzitter Stichting De Vrije Huisarts
Dhr. D. Schravendeel, Het Expertise Centrum
Dr. E. Schreuders, directeur/adviseur Net2Legal privacyadvies
Dhr. C.J.M. Schuyt, staatsraad van het Koninkrijk, Raad van State
Dhr. W. Sijstermans, CIO bij ministerie van Financiën
Dhr. W. van Sluijs, Permanente Vertegenwoordiging bij de EU, Brussel
Dhr. L.J.E. Smits, directeur Het Expertise Centrum
Mevr. M. Smits, Rathenau Instituut
Dhr. B. Smals, hoofdbestuurslid KNMP en apotheker
Prof. I. Snellen, emeritus hoogleraar Bestuurskunde, EUR
Dhr. E.-J. Sol, TNO
Mevr. K. Spaink, columnist/XS4ALL internet
Mevr. A. Sprokkereef, Visiting Researcher TILT, Universiteit van Tilburg

Dhr. J. Stam, ministerie van Justitie
Dhr. J. van den Steenhoven, Stichting Nederland Kennisland
Dhr. K. van der Steenhoven, CIO bij ministerie van OC&W
Dhr. H. van der Stelt, CIO bij ministerie van V&W
Mevr. N. Stolk-Luyten, CIO bij ministerie van BZK
Mevr. S. J. Stuiveling, president van de Algemene Rekenkamer
Mevr. prof. M. Sturkenboom, Professor of Pharmaco-epidemiology, Erasmus Universiteit Rotterdam
Dhr. prof. K. Stuurman, hoogleraar Normering van Informatietechnologie, Universiteit van Tilburg; partner ICT-recht Van Doorne N.V.
Mevr. I.Y. Tan, lid Eerste Kamer
Dhr. H. Tankink, waarnemend directeur Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR)
Dhr. F. Teeven, lid Tweede Kamer voor de VVD
Dhr. prof. M. Thaens, HEC/ROI/hoogleraar ICT en strategisch innoveren in de publieke sector, EUR
Dhr. C.P. Thissen, lid Eerste Kamer
Dhr. A. Thijssen, directeur Dienstverlening, Regeldruk en Informatiebeleid, ministerie van BZK
Dhr. K. Thomeer, huisarts te Hulst en Geneesheer-Specialist beheer van gezondheidsgegevens te België
Mevr. M. Timmer, Ketenmanager Veiligheidshuis Zaanstreek-Waterland
Mevr. T. Timmermans, ministerie van BZK
Dhr. R. van Troost, NVVB
Dhr. J.J.M. Uijlenbroek, directeur-generaal Organisatie en Bedrijfsvoering Rijk, ministerie van BZK
Dhr. A. Vedder, Universitair hoofddocent TILT, Universiteit van Tilburg
Dhr. T. Veenstra, CIO bij ministerie van EZ
Mevr. S. in 't Veld, lid Europees Parlement
M.D. van de Velde, projectadviseur Meldpunt Identiteitsfraude i.o., Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR)
Dhr. W. van Vemde, korpschef Politie Gooi en Vechtstreek, portefeuillehouder ID, Raad van Hoofdcommissarissen
Dhr. M. Verhagen, plaatsvervangend directeur ICT en Toepassing bij het ministerie van Economische Zaken
Dhr. prof. Ch. Verhoef, hoogleraar IT governance Vrije Universiteit Amsterdam
Dhr. J. Verschuur, directeur ICT Leadership Ernst & Young
Dhr. C. Versluis, Sociale Verzekeringsbank
Dhr. K. Versmissen, ID-wise
Dhr. R. Verweij, RINIS
Dhr. A. Vlug, manager Ontwerp en Onderhoud, Nictiz
Mevr. G. Vogel, projectleider EKD, Twente
Dhr. G. Wabeke, manager Justitieel Aftappen & Monitoren KPN

Dhr. P. Waters, hoofd Bureau Forum Standaardisatie
Dhr. W. Wensink, PriceWaterhouseCoopers
Dhr. H. Wesseling, CIO bij TNT/lid CIO-overleg
Dhr. E. Whitley, London School of Economics
Mevr. M. Wijnstok, coördinerend beleidsmedewerker, projectleider i-visie, Landbouw, Natuur & Voedselkwaliteit
Mr. P.J. Wijntje, directoraat-generaal Belastingdienst, ministerie van Financiën
Dhr. C. de Wijs, Logica
Dhr. Th. Wijsman, Algemene Rekenkamer
Dhr. H. Woltring, Zorg Voor Jeugd/Matchpoint
Dhr. P. van der Zanden, ministerie van Buitenlandse Zaken
Mevr. D. Zinberg, Harvard University, Verenigde Staten
Dhr. prof. A. Zuurmond, hoogleraar ICT en de toekomst van het openbaar bestuur, Technische Universiteit Delft, partner Zenc
Dhr. H. Zwijnenberg, TNO

RAPPORTEN AAN DE REGERING

Eerste raadsperiode (1972-1977)

1 Europese Unie
2 Structuur van de Nederlandse economie
3 Energiebeleid
Gebundeld in één publicatie (1974)
4 Milieubeleid (1974)
5 Bevolkingsgroei (1974)
6 De organisatie van het openbaar bestuur (1975)
7 Buitenlandse invloeden op Nederland: Internationale migratie (1976)
8 Buitenlandse invloeden op Nederland: Beschikbaarheid van wetenschappelijke en technische kennis (1976)
9 Commentaar op de Discussienota Sectorraden (1976)
10 Commentaar op de nota Contouren van een toekomstig onderwijsbestel (1976)
11 Overzicht externe adviesorganen van de centrale overheid (1976)
12 Externe adviesorganen van de centrale overheid (1976)
13 Maken wij er werk van? Verkenningen omtrent de verhouding tussen actieven en niet-actieven (1977)
14 Interne adviesorganen van de centrale overheid (1977)
15 De komende vijfentwintig jaar – Een toekomstverkenning voor Nederland (1977)
16 Over sociale ongelijkheid – Een beleidsgerichte probleemverkenning (1977)

Tweede raadsperiode (1978-1982)

17 Etnische minderheden (1979)
A. Rapport aan de Regering
B. Naar een algemeen etnisch minderhedenbeleid?
18 Plaats en toekomst van de Nederlandse industrie (1980)
19 Beleidsgerichte toekomstverkenning
Deel 1: Een poging tot uitlokking (1980)
20 Democratie en geweld. Probleemanalyse naar aanleiding van de gebeurtenissen in Amsterdam op 30 april 1980
21 Vernieuwingen in het arbeidsbestel (1981)
22 Herwaardering van welzijnsbeleid (1982)
23 Onder invloed van Duitsland. Een onderzoek naar gevoeligheid en kwetsbaarheid in de betrekkingen tussen Nederland en de Bondsrepubliek (1982)
24 Samenhangend mediabeleid (1982)

Derde raadsperiode (1983-1987)

25 Beleidsgerichte toekomstverkenning
Deel 2: Een verruiming van perspectief (1983)
26 Waarborgen voor zekerheid. Een nieuw stelsel van sociale zekerheid in hoofdlijnen (1985)
27 Basisvorming in het onderwijs (1986)
28 De onvoltooide Europese integratie (1986)
29 Ruimte voor groei. Kansen en bedreigingen voor de Nederlandse economie in de komende tien jaar (1987)
30 Op maat van het midden- en kleinbedrijf (1987)

Deel 1: Rapport aan de Regering

Deel 2: Pre-adviezen

31 Cultuur zonder grenzen (1987)

32 De financiering van de Europese Gemeenschap. Een interimrapport (1987)

33 Activerend arbeidsmarktbeleid (1987)

34 Overheid en toekomstonderzoek. Een inventarisatie (1988)

Vierde raadsperiode (1988-1992)

35 Rechtshandhaving (1988)

36 Allochtonenbeleid (1989)

37 Van de stad en de rand (1990)

38 Een werkend perspectief. Arbeidsparticipatie in de jaren '90 (1990)

39 Technologie en overheid (1990)

40 De onderwijsverzorging in de toekomst (1991)

41 Milieubeleid. Strategie, instrumenten en handhaafbaarheid (1992)

42 Grond voor keuzen. Vier perspectieven voor de landelijke gebieden in de Europese Gemeenschap (1992)

43 Ouderen voor ouderen. Demografische ontwikkelingen en beleid (1993)

Vijfde raadsperiode (1993-1997)

44 Duurzame risico's. Een blijvend gegeven (1994)

45 Belang en beleid. Naar een verantwoorde uitvoering van de werknemersverzekeringen (1994)

46 Besluiten over grote projecten (1994)

47 Hoger onderwijs in fasen (1995)

48 Stabiliteit en veiligheid in Europa. Het veranderende krachtenveld voor het buitenlands beleid (1995)

49 Orde in het binnenlands bestuur (1995)

50 Tweedeling in perspectief (1996)

51 Van verdelen naar verdienen. Afwegingen voor de sociale zekerheid in de 21e eeuw (1997)

52 Volksgezondheidszorg (1997)

53 Ruimtelijke-ontwikkelingspolitiek (1998)

54 Staat zonder land. Een verkenning van bestuurlijke gevolgen van informatie- en communicatietechnologie (1998)

Zesde raadsperiode (1998-2002)

55 Generatiebewust beleid (1999)

56 Het borgen van publiek belang (2000)

57 Doorgroei van arbeidsparticipatie (2000)

58 Ontwikkelingsbeleid en goed bestuur (2001)

59 Naar een Europabrede Unie (2001)

60 Nederland als immigratiesamenleving (2001)

61 Van oude en nieuwe kennis. De gevolgen van ICT voor het kennisbeleid (2002)

62 Duurzame ontwikkeling. Bestuurlijke voorwaarden voor een mobiliserend beleid (2002)

63 De toekomst van de nationale rechtsstaat (2002)

64 Beslissen over biotechnologie (2003)

65 Slagvaardigheid in de Europabrede Unie (2003)

66 Nederland handelsland. Het perspectief van de transactiekosten (2003)
67 Naar nieuwe wegen in het milieubeleid (2003)

Zevende raadsperiode (2003-2007)

68 Waarden, normen en de last van het gedrag (2003)
69 De Europese Unie, Turkije en de islam (2004)
70 Bewijzen van goede dienstverlening (2004)
71 Focus op functies. Uitdagingen voor een toekomstbestendig mediabeleid (2005)
72 Vertrouwen in de buurt (2005)
73 Dynamiek in islamitisch activisme. Aanknopingspunten voor democratisering en mensenrechten (2006)
74 Klimaatstrategie – tussen ambitie en realisme (2006)
75 Lerende overheid. Een pleidooi voor probleemgerichte politiek (2006)
76 De verzorgingsstaat herwogen. Over verzorgen, verzekeren, verheffen en verbinden (2006)
77 Investeren in werkzekerheid (2007)
78 Europa in Nederland (2007)
79 Identificatie met Nederland (2007)
80 Innovatie vernieuwd. Opening in viervoud (2008)
81 Infrastructures. Time to Invest (2008)

Achtste raadsperiode (2008-2012)

82 Onzekere veiligheid. Verantwoordelijkheden rond fysieke veiligheid (2008)
83 Vertrouwen in de school. Over de uitval van 'overbelaste' jongeren (2009)
84 Minder pretentie, meer ambitie. Ontwikkelingshulp die verschil maakt (2010)
85 Aan het buitenland gehecht. Over verankering en strategie van Nederlands buitenlandbeleid (2010)

Rapporten aan de Regering nrs. 1 t/m 67 en publicaties in de reeks *Voorstudies en achtergronden* zijn niet meer leverbaar. Alle studies van de WRR zijn beschikbaar via de website www.wrr.nl.
Rapporten aan de Regering nrs. 68 t/m 85 zijn verkrijgbaar in de boekhandel of via Amsterdam University Press, Herengracht 221, 1016 BG Amsterdam (www.aup.nl).

VERKENNINGEN

Zevende raadsperiode (2003-2007)

1 J. Pelkmans, M. Sie Dhian Ho en B. Limonard (red.) (2003) Nederland en de Europese grondwet
2 P.T. de Beer en C.J.M. Schuyt (red.) (2004) Bijdragen aan waarden en normen
3 G. van den Brink (2004) Schets van een beschavingsoffensief. Over normen, normaliteit en normalisatie in Nederland
4 E.R. Engelen en M. Sie Dhian Ho (red.) (2004) De staat van de democratie. Democratie voorbij de staat
5 P.A. van der Duin, C.A. Hazeu, P. Rademaker en I.J. Schoonenboom (red.) (2004) Vijfentwintig jaar later. De Toekomstverkenning van de WRR uit 1977 als leerproces
6 H. Dijstelbloem, P.L. Meurs en E.K. Schrijvers (red.) (2004) Maatschappelijke dienstverlening. Een onderzoek naar vijf sectoren
7 W.B.H.J. van de Donk, D.W.J. Broeders en F.J.P. Hoefnagel (red.) (2005) Trends in het medialandschap. Vier verkenningen
8 G. Engbersen, E. Snel en A. Weltevrede (2005) Sociale herovering in Amsterdam en Rotterdam. Eén verhaal over twee wijken
9 D.J. Wolfson (2005) Transactie als bestuurlijke vernieuwing. Op zoek naar samenhang in beleid en uitvoering
10 Nasr Abu Zayd (2006) Reformation of Islamic Thought. A Critical Historical Analysis
11 J.M. Otto (2006) Sharia en nationaal recht. Rechtssystemen in moslimlanden tusssen traditie, politiek en rechtsstaat
12 P.L. Meurs, E.K. Schrijvers en G.H. de Vries (red.) (2006) Leren van de praktijk. Gebruik van lokale kennis en ervaring voor beleid
13 W.B.H.J. van de Donk, A.P. Jonkers en G.J. Kronjee (red.) (2006) Geloven in het publieke domein. Verkenningen van een dubbele transformatie
14 D. Scheele, J.J.M. Theeuwes, G.J.M. de Vries (red.) (2007) Arbeidsflexibiliteit en ontslagrecht
15 P.A.H. van Lieshout, M.S.S. van der Meij en J.C.I. de Pree (red.) (2007) Bouwstenen voor betrokken jeugdbeleid
16 J.J.C. Voorhoeve (2007) From War to the Rule of Law. Peace Building after Violent Conflicts
17 M. Grever en K. Ribbens (2007) Nationale identiteit en meervoudig verleden
18 B. Nooteboom and E. Stam (eds.) (2008) Micro-foundations for Innovation Policy
19 G. Arts, W. Dicke and L. Hancher (eds.) (2008) New Perspectives on Investments in Infrastructures

Achtste raadsperiode (2008-2012)

20 D. Scheele, R. van Gaalen en J. van Rooijen (2008) Werk en inkomsten na massaontslag: de zekerheid is niet van de baan
21 Monique Kremer, Peter van Lieshout and Robert Went (eds.) (2009) Doing Good or Doing Better. Development Policies in a Globalizing World
22 W.L. Tiemeijer, C.A. Thomas en H.M. Prast (red.) (2009) De menselijke beslisser. Over de psychologie van keuze en gedrag
23 Huub Dijstelbloem, Paul den Hoed, Jan Willem Holtslag en Steven Schouten (red.) (2010) Het gezicht van de publieke zaak. Openbaar bestuur onder ogen
24 M.B.A. van Asselt, A. Faas, F. van der Molen en S.A. Veenman (red.) (2010) Uit zicht. Toekomstverkennen met beleid
25 D. Broeders, C.M.K.C. Cuijpers en J.E.J. Prins (red.) (2011) De staat van informatie

Alle *Verkenningen* zijn verkrijgbaar in de boekhandel of via Amsterdam University Press, Herengracht 221, 1016 BG Amsterdam (www.aup.nl).

WEBPUBLICATIES

Zevende raadsperiode (2003-2007)

WP 01 Opvoeding, onderwijs en jeugdbeleid in het algemeen belang
WP 02 Ruimte voor goed bestuur: tussen prestatie, proces en principe
WP 03 Lessen uit corporate governance en maatschappelijk verantwoord ondernemen
WP 04 Regulering van het bestuur van maatschappelijke dienstverlening: eenheid in verscheidenheid
WP 05 Een schets van het Europese mediabeleid
WP 06 De regulering van media in internationaal perspectief
WP 07 Beleid inzake media, cultuur en kwaliteit: enkele overwegingen
WP 08 Geschiedenis van het Nederlands inhoudelijk mediabeleid
WP 09 Buurtinitiatieven en buurtbeleid in Nederland anno 2004: analyse van een veldonderzoek van 28 casussen
WP 10 Geestelijke gezondheid van adolescenten: een voorstudie
WP 11 De transitie naar volwassenheid en de rol van het overheidsbeleid: een vergelijking van institutionele arrangementen in Nederland, Zweden, Groot-Brittanië en Spanje
WP 12 Klassieke sharia en vernieuwing
WP 13 Sharia en nationaal recht in twaalf moslimlanden
WP 14 Climate strategy: Between ambition and realism
WP 15 The political economy of European integration in the polder: Asymmetrical supranational governance and the limits of legitimacy of Dutch EU policy-making
WP 16 Europe in law, law in Europe
WP 17 Faces of Europe: Searching for leadership in a new political style
WP 18 The psychology and economics of attitudes in the Netherlands
WP 19 Citizens and the legitimacy of the European Union
WP 20 No news is bad news! The role of the media and news framing in embedding Europe
WP 21 Actor paper subnational governments: Their role in bridging the gap between the EU and its citizens
WP 22 The Dutch third sector and the European Union: Connecting citizens to Brussels
WP 23 Europe in parliament: Towards targeted politicization
WP 24 Europe in the Netherlands: Political parties
WP 25 The EU Constitutional Treaty in the Netherlands: Could a better embedding have made a difference?
WP 26 How to solve the riddle of belated Euro contestation in the Netherlands?
WP 27 Connection, consumer, citizen: Liberalising the European Union gas market
WP 28 Dutch EU-policies with regard to legal migration – The directive on family reunification
WP 29 The accession of Turkey to the European Union: The political decision-making process on Turkey in The Netherlands
WP 30 The Habitats Directive: A case of contested Europeanization
WP 31 Encapsulating services in the 'polder': Processing the Bolkestein Directive in Dutch Politics
WP 32 Zorgen over de grens
WP 33 De casus Inburgering en Nationaliteitswetgeving: iconen van nationale identiteit
WP 34 In debat over Nederland

Achtste raadsperiode (2008-2012)

WP 35 Veel voorkomende criminaliteit
WP 36 Gevaarlijke stoffen
WP 37 ICT en internet
WP 38 Voedsel en geneesmiddelen
WP 39 Waterbeheer en waterveiligheid
WP 40 Verschuivende vensters: veranderingen in het institutionele landschap van de Nederlandse ontwikkelingssamenwerking
WP 41 Internationale publieke goederen: karakteristieken en typologie
WP 42 Het Nederlandse veiligheidsbeleid in een veranderende wereld
WP 43 Internationalisering en Europeanisering van strafrechtelijke rechtshandhaving in Nederland
WP 44 Praktijken van beleidsgerichte toekomstverkenning : een inventarisatie
WP 45 Het landelijk EPD als blackbox: besluitvorming en opinies in kaart
WP 46 Happy Landings? Het biometrische paspoort als zwarte doos
WP 47 Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit
WP 48 eCall Blackbox
WP 49 Blackbox-onderzoek veiligheidshuizen
WP 50 Goed opdrachtgeverschap jegens ICTU
WP 51 Het biometrische paspoort in Nederland: crash of zachte landing?
WP 52 De prijs van heupen en knieën
WP 53 Vitaal en bevlogen
WP 54 Procedures en problemen op de markt voor reïntegratiedienstverlening
WP 55 Securization in the Netherlands shaped by and shaping regulation
WP 56 Hallmarking Halal
WP 57 Markets and public values in healthcare
WP 58 Het buitenlandse beleid van middelgrote mogendheden
WP 59 'Location based privacy' in constellaties van publiek-private verantwoordelijkheid

WRR RAPPORTEN AAN DE REGERING 86

iOverheid

Het biometrisch paspoort, de Verwijsindex Risicojongeren, het Elektronisch Patiëntendossier, nationale en internationale gegevensuitwisseling tussen organisaties of het gebruik van digitale profielen van burgers: deze en vele andere toepassingen staan beleidsmakers en uitvoerders ter beschikking dankzij de inzet van ICT.

Maar wat betekent de inzet van ICT in beleid en uitvoering voor de relatie tussen overheid en burgers? Wat zijn de gevolgen voor het functioneren van de overheid zelf? Hoe wordt in het proces van voortgaande digitalisering een afweging gemaakt tussen beginselen als veiligheid, privacy, efficiëntie en transparantie?

In dit rapport concludeert de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) dat in de dagelijkse digitale praktijk een iOverheid is ontstaan die volop 'draait' op nieuwe informatiestromen die door ICT mogelijk zijn gemaakt. Die nieuwe iOverheid loopt echter flink uit de pas met de bestaande structuur en de verantwoordelijkheden van de overheid. De WRR doet in dit rapport inhoudelijke en institutionele aanbevelingen om de noodzakelijke paradigmawisseling van eOverheid naar iOverheid in goede banen te leiden.

9 789089 643094 >

ISBN 978 90 8964 309 4

Amsterdam University Press • www.aup.nl